RFID-Recht der Zukunft

Brauchen wir in einer ubiquitären Radiofrequenz-Umgebung bereichsspezifische Datenschutzregelungen zur Verhinderung der Erosion der Rechte des Einzelnen?

Vom Fachbereich Rechts- und Wirtschaftswissenschaften der
Technischen Universität Darmstadt genehmigte

Dissertation

zur Erlangung des akademischen Grades eines Doctor iuris (Dr. iur.)

Vorgelegt von

Ass. iur. Franziska Löw, LL.M.

Geburtsdatum: 24.01.1983
Geburtsort: Seeheim-Jugenheim

Erstgutachterin: Prof. Dr. Viola Schmid, LL.M. (Harvard)
Zweitgutachter: Prof. Dr. Jochen Marly

Eingereicht am: 2. Mai 2012
Mündliche Prüfung am: 11. Februar 2013
Darmstadt 2013
D 17

Inhalt

A. Einleitung

I. Untersuchungsgegenstand

Folgende Thesen werden in dieser Arbeit untersucht:

- RFID wird sich als ubiquitäre Technologie etablieren, auch wenn sie die an sie gestellten Prognosen der letzten Jahre noch nicht erfüllt hat.
- Mit seinen technologischen Besonderheiten stellt RFID das Datenschutzrecht bereits jetzt vor neue, in dieser Form noch nicht dagewesene Herausforderungen. Insbesondere die bisherige Auslegung des Begriffs „personenbezogene Daten“ stößt in RFID-Szenarien an ihre Grenzen. Mit zunehmender Verbreitung der Technik werden diese Herausforderungen dringlicher.
- Der in der EU und Deutschland bestehende datenschutzrechtliche Rahmen ist theoretisch geeignet, auf Datenschutzherausforderungen im Zusammenhang mit RFID zu reagieren.[1] In der Praxis wird er diesem Anspruch indes nicht gerecht: Das traditionelle Datenschutzrecht ist der Dynamik neuer technischer Entwicklungen wie RFID nicht gewachsen.
- Die auf EU-Ebene bereits eingeführten Maßnahmen (Empfehlung der Kommission) werden nicht ausreichen, um einen hinreichenden Schutz für das Recht auf informationelle Selbstbestimmung zu gewährleisten.
- Spezialgesetzliche Regelungen, wie in den USA diskutiert, können auch in der EU als Vorbild für gesetzgeberische Maßnahmen dienen, sie sollten aber nur eine ergänzende Funktion zu den allgemeinen, technikneutral gestalteten Datenschutzregelungen der EU und Deutschland haben.
- Im Rahmen des weiteren Verlaufs der Debatte um RFID-Datenschutz wird notwendigerweise zunächst das Konzept des Begriffs der personenbezogenen Daten überdacht und an die gegebenen Herausforderungen angepasst werden müssen.
- Um einen effektiven Schutz des informationellen Selbstbestimmungsrechts in einer zunehmend technisierten Umgebung mit ubiquitärer RFID-Infrastrukturen erreichen

[1] In dieser Arbeit wird das Thema Arbeitnehmerdatenschutz in RFID-Anwendungen ausgeklammert. Dieser aufgrund des großen Betroffenenkreises sehr wichtige Aspekt bei der datenschutzrechtlichen Bewertung von RFID-Szenarien bedarf eigenständiger wissenschaftlicher Untersuchung. Dies zeigt sich nicht zuletzt an der Vielzahl der in dieser Legislaturperiode eingebrachten Gesetzesinitiativen zum Beschäftigtendatenschutz. Neben der Bundesregierung (BTDrucks 17/4230, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf (04.04.2013) haben auch die Fraktionen der SPD (BTDrucks 17/69, abrufbar unter http://dip21.bundestag.de/dip21/btd/17/000/1700069.pdf (04.04.1013) und der GRÜNEN (BTDrucks 17/4853, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/048/1704853.pdf (04.04.2013) jeweils einen Gesetzentwurf in den Bundestag eingebracht. Zum Zeitpunkt der Veröffentlichung ist keiner der Entwürfe verabschiedet worden.

Auch eine vertiefte Untersuchung der rechtlichen Vorschriften für die Verwendung von RFID in Betreuungssituationen erfolgt in dieser Arbeit nicht. Als spezieller Anwendungsfall für RFID bleiben die Herausforderungen, die RFID an das Betreuungsrecht stellt, eigener wissenschaftlicher Auseinandersetzung vorbehalten.

zu können, ist es erforderlich, dem Einzelnen mehr Einfluss auf den Umgang mit den eigenen personenbezogenen Daten zu geben. Hierfür muss wesentlich mehr Transparenz geschaffen werden.

- Der von der EU-Empfehlung aufgegriffene „Privacy-by-Design"-Ansatz wird neben der Stärkung der Einflussmöglichkeiten des Einzelnen auf den Umgang mit seinen personenbezogenen Daten ein wesentlicher Baustein in einem künftigen RFID-Datenschutzkonzept sein.
- Selbstregulierungskonzepte können und sollten von der Wirtschaft eingesetzt werden. Sie entbinden den Staat aber nicht von seiner Handlungspflicht.
- Ein weiteres Aufschieben der erforderlichen gesetzgeberischen Maßnahmen schürt Unsicherheiten bei allen Beteiligten – Verbrauchern, Wirtschaft, Rechtsanwendern – und hemmt damit die Entwicklung und Verbreitung der Technologie eher, als dass es sie fördert.

II. Vorgehensweise

Die Arbeit wird sich zunächst – Teil B – mit einigen Grundlagen befassen, deren Kenntnis erforderlich für das Verständnis der datenschutzrechtlichen Herausforderungen von RFID ist. Als erstes werden daher die allgemeinen technischen Vorgaben von RFID-Systemen dargestellt. Im Anschluss werden die unterschiedlichen Anwendungsbereiche für RFID erörtert.

Den verschiedenen Anwendungen werden in Teil C Szenarien gegenüber gestellt. Die Anwendungsbereiche unterfallen alle einem oder auch mehreren dieser Szenarien, die unterschiedliche Herausforderungen an das geltende Recht stellen. Zum Abschluss von Teil C werden vier *Leading Scenarios* herausgearbeitet, anhand derer der bestehende Datenschutzrechtsrahmen auf seine Wirksamkeit in RFID-Anwendungen untersucht wird.

Diese Untersuchung anhand der *Leading Scenarios* wird in Teil D vorgenommen. Berücksichtigung findet hierbei sowohl Rechtsrahmen der EU als auch der deutsche Rechtsrahmen. Hierbei werden zunächst der europäische sowie der verfassungsrechtliche Rahmen dargestellt, auf dessen Grundlage das einfachgesetzliche deutsche Datenschutzrecht beruht. Letzteres wird dann anhand seiner vorgegebenen Struktur auf seine Wirksamkeit zur Bewältigung der bestehenden und zu erwartenden Herausforderungen im Rahmen der herausgearbeiteten *Leading Scenarios* untersucht.

In Teil E geht die Arbeit auf die Entwicklungen zur Schaffung RFID-spezifischen Datenschutzrechts ein. Hierbei wird zunächst auf die europäischen Vorgaben – maßgeblich die Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen[2] – und deren Handhabung und Umsetzung in Deutschland eingegangen. In einem weiteren Schritt werden die Entwicklungen in

[2] Europäische Kommission, Empfehlung 2009/387/EG vom 12.05.2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen, ABl. L 122/47 vom 16.05.2009, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF (04.04.2013).

den USA dargestellt und auf eine etwaige Vorbildeigenschaft für die europäischen Gesetzgeber untersucht.

Nach einer Bewertung der Erkenntnisse in Teil F wird die Arbeit im Rahmen eines Ausblicks in Teil G Handlungsempfehlungen an den Gesetzgeber, die Branche sowie die Endnutzer formulieren, die als Leitfaden für einen weiteren Umgang mit RFID gesehen werden können.

B. Grundlagen

I. Definition und Technische Grundlagen

Um zu verstehen, warum bei Verwendung von RFID datenschutzrechtliche Herausforderungen die Folge sein können, ist die Kenntnis der grundlegenden technischen Funktionsweise von RFID erforderlich. Diese soll im Folgenden dargestellt werden.

1. Definition Radiofrequenzidentifikation (RFID)

Eine allgemein anerkannte Definition für RFID gibt es nicht. Dies rührt nicht zuletzt daher, dass unter den Begriff verschiedene Techniken fallen, die sich aber in ihrer grundlegenden Funktionsweise gleichen. Gemein haben sie alle, dass über die Auslesung von Daten aus einem Transponder mittels Radiowellen die Identifikation von Gegenständen oder Personen ermöglicht wird. Eine solche spezielle Technik ist z.B. „Near Field Communication“ (NFC), die verbreitet Einsatz in Mobiltelefonen aber auch in den neuen Pässen und Personalausweisen findet.[3]

Die Europäische Kommission hat im Mai 2009 eine Empfehlung[4] veröffentlicht, in der sie die ersten rechtlichen Vorgaben für den Einsatz von RFID trifft.[5] In Punkt 3 a) der Empfehlung definiert die Kommission RFID für die Zwecke der Empfehlung:

> „Funkwellenidentifikation“ (RFID) ist die Nutzung elektromagnetischer Wellen oder der elektromagnetischen Nachfeldkopplung im Funkbereich des Frequenzspektrums für die Kommunikation von oder zu einem RFID-Tag mit Hilfe verschiedener Modulations- oder Kodierungstechniken oder nur für das Auslesen der Kennung eines RFID-Tags oder anderer darin gespeicherter Daten;

In einem aktuellen Gesetzesvorschlag im Staat New York, USA zu einem „RFID *Right to Know-Act*“ findet sich folgende Definition:

> „Radio Frequency Identification” means any technology that uses radio waves or other wireless means to transmit identifying information between a tag, badge or other device and a reader without physical contact.[6]

Maßgeblich ist in allen Fällen das Vorliegen folgender Parameter:

- Zwischen einem Transponder (Tag, Chip etc.) und
- einem Lesegerät wird

---

[3] Hierzu unten mehr, Teil B.I.2.b)dd).

[4] Europäische Kommission, Empfehlung 2009/387/EG, oben Fn. 2.

[5] Weil eine Empfehlung der Kommission keine Bindungswirkung in den Mitgliedstaaten hat, vgl. § 288 Abs. 5 AEUV (ex.-Art. 249 EG), weist die Definition keinen rechtlich verbindlichen Charakter auf.

[6] New York 2011 A.B. 1033, A.B. 8428 sowie S.B. 1168 – A.B. steht für „Assembly Bill” und S.B. für „Senate Bill“, einsehbar auf der offiziellen „Bill Search“ Seite der New York State Assembly, abrufbar unter http://assembly.state.ny.us/leg/ (04.04.2013). Übersetzung (der Autorin): „Radiofrequenzidentifikation“ meint jede Technologie, die Radiowellen oder andere drahtlose Mittel zur Übermittlung von Identifikationsinformationen zwischen einem Etikett, einer Marke oder einem sonstigen Gerät und einem Lesegerät ohne Verwendung physikalischen Kontakts verwendet.“; eine Recherche zu den Bestrebungen der Gesetzgeber auf U.S. Staatenebene bereichsspezifische RFID-Gesetze zu erlassen hat 2007 bereits vorgenommen *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 202.

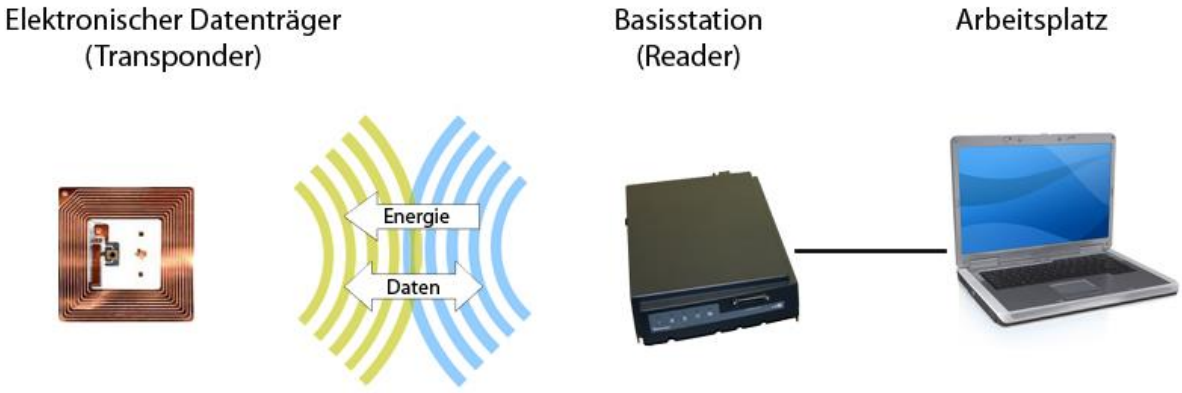
- ohne physischen Kontakt
- über Distanz
- mittels Funk- oder elektromagnetischer Wellen
- ein Kommunikationsvorgang generiert, bei dem
- auf dem Transponder gespeicherte (Identifikations-)Daten
- ausgelesen bzw. in sonstiger Weise bearbeitet werden.

2. RFID-Technik

RFID[7] weist im Vergleich zu anderen bereits bekannten Identifikationssystemen wie Barcode oder Chipkarten die Besonderheit auf, dass kein visueller bzw. sonstiger physischer Kontakt mehr zum Auslesen der Daten erforderlich ist. Die Daten werden per Radiosignal übertragen.

Jedes RFID-gestützte System besteht aus drei Komponenten:

- einem Transponder/Chip, auch "Tag" genannt,
- einem Lesegerät, dem "Reader", und
- einem dahinter stehenden die Daten verarbeitenden Computersystem, dem „Backend“.



Quelle: Logistik-Service-Bus, abrufbar unter http://www.lsb-plattform.de/rfid-labor (04.04.2013)

Bei dem Tag handelt es sich um einen Chip, der entweder auf den zu identifizierenden Gegenstand appliziert oder aber in ihn implementiert werden kann. Bei letzterer Vorgehensweise spricht man auch von *embedded systems*, also „eingebauten Systemen“. Solche Systeme finden sich bereits heute überall, wo Mikroprozessoren in Alltagsgegenstände integriert sind. So zum Beispiel bei Autos, Nähmaschinen, Heimtrainern, Fotokopiergeräten u.ä.[8] Bereits verbreitete *embedded systems* stellen allerdings nur den Vorläufer zu RFID-gestützten Systemen dar. Mikroprozessoren alleine machen Produkte noch nicht zu *smart things*, wie es bei der Verwendung von RFID zu erwarten sein wird. Ziel von RFID ist die Implementierung eines einzigen kleinen bis kleinsten Transponders, der gegebenenfalls sogar Umgebungsparameter

[7] Für die Arbeit war es wichtig, die grundlegenden technischen Voraussetzungen von RFID-Systemen darzustellen. Aufgrund der eingeschränkten technischen Expertise der Verfasserin wurde auf einschlägige Literatur zurückgegriffen. Die Beiziehung eines technischen Experten hat nicht stattgefunden.

[8] *Mattern*, Die technische Basis für das Internet der Dinge *in*: Fleisch/Mattern (Hrsg.), Das Internet der Dinge, S. 61.

wahrnehmen kann, diese verarbeitet und bei Bedarf sofort an ein Lesegerät und dann an ein angeschlossenes IT-System weitergibt.[9]

Die Identifizierung von Personen kann entweder über einen mitgeführten getaggten Gegenstand erfolgen – z.B. einer Kundenkarte – oder aber, indem ein RFID-Tag direkt implantiert wird.

a) RFID Transponder – „Tag“

RFID-Tags sind kleine bis winzige Speicherchips – denkbar ist die Herstellung von Chips in der Größe von Staubkörnern. Typischerweise ist das Tag ausgestattet mit einem Mikrochip und einer Kopplungseinheit. Je nach Technologie unterscheidet man zwischen Tags, die entweder eine Spule oder eine Antenne als Kopplungseinheit haben.[10] Die Chips enthalten mindestens einen Radio-Empfänger, um die Signale des Readers empfangen zu können, einen Radio-Modulator, um entsprechende Antwort-Signale an den Reader zurückzusenden, ein Mindestmaß an Speicherkapazität, ein Energiesystem – teils mit eigener Energiequelle – sowie einen Prozessor.[11]

RFID-Tags können in verschiedensten Formen hergestellt werden.[12] Je nach Einsatzgebiet werden Chips in runder oder eckiger Form produziert, die in Glas-, Plastik- oder Ferritgehäuse eingebaut oder auf flexible Klebefolien aufgebracht werden. Letztere Tags nennt man auch *Smart Labels*.[13] RFID-Tags können durch die verschiedenen Erscheinungsformen in unterschiedlichste Gegenstände eingebracht werden, z.B. in Uhren, in Chipkarten, die Implantierung direkt unter die Haut (bei Tieren, aber auch ein Tagging von Menschen ist mittels Glasröhrchen-Transponder denkbar) oder die Applikation auf Metall- oder Glasflächen.

Zu unterscheiden sind drei Arten von Tags: passive, semi-aktive und aktive. Passive Tags zeichnen sich durch geringe Herstellungskosten aus. Nachteil ist, dass sie nicht mit einer eigenen Energieversorgung ausgestattet sind. Semi-aktive Tags haben bereits eine eigene Energiequelle, sie verwenden aber die durch das elektromagnetische Feld des Lesegeräts übermittelte Energie für die Antwort an das Lesegerät.[14] Aktive Tags verfügen regelmäßig über einen größeren Speicher, sind mit einer eigenen Batterie versehen, kosten aber im Gegenzug auch mehr in der Herstellung.

---

[9] *Mattern*, Die technische Basis für das Internet der Dinge *in*: Fleisch/Mattern (Hrsg.), Das Internet der Dinge, S. 62.

[10] *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 71.

[11] *Garfinkel/Holtzman*, Understanding RFID Technology *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 17; *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 163.

[12] Vgl. zu den verschiedenen Herstellungsformen *Finkenzeller*, RFID Handbuch, S. 14 ff., 377 ff.

[13] *Finkenzeller*, RFID-Handbuch, S. 21.

[14] *Garfinkel/Holtzman*, Understanding RFID Technology *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 17; *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 73.

Unterschiedliche Anwendungsbereiche erfordern hierbei unterschiedliche technische Ausgestaltungen. Geht es darum, ein Produkt eindeutig identifizieren zu können, benötig man lediglich eine einzigartige Identifikationsnummer auf dem Tag. Um eine solche zu speichern und abrufen zu können, genügt regelmäßig ein passives Tag. Sollen auf dem Tag hingegen mehr Informationen gespeichert werden, etwa Ort und Zeitpunkt der Herstellung, Lieferweg, Bestimmungsort und Inhalt eines Produkts, oder sogar Sensortechnik verwendet werden, muss das Tag über entsprechende Speicherkapazitäten und Rechenleistungen verfügen, sodass hier aktive Tags zum Einsatz kommen.

aa) Passive Tags

Passive RFID-Tags sind wesentlich viel kleiner als aktive. Dies alleine schon deshalb, weil sie über keine eigene Energieversorgung verfügen. Sie befinden sich solange im Standby-Modus, bis sie von einem Reader in Reichweite aktiviert werden. Das magnetische oder elektromagnetische Feld, das das Lesegerät generiert, versorgt das Tag mit der erforderlichen Energie und ermöglicht die Rücksendung der Antwort.[15]

Aufgrund der technisch wesentlich viel einfacheren Gestaltung passiver Tags, sind diese in der Herstellung um ein vielfaches günstiger. Die Herstellungskosten pro Stück belaufen sich bereits heute auf wenige Cents und es ist zu erwarten, dass im Zuge von Massenherstellung die Kosten weiter sinken werden.[16]

Ohne Energieversorgung ist die Sendereichweite von RFID-Tags nicht sonderlich groß. Erforderlich für ein erfolgreiches Auslesen der Daten ist demnach, dass Tag und Reader in engen physischen Kontakt treten. Manche Tags haben lediglich Sendereichweiten von wenigen Zentimetern.

Bei passiven Tags ist eine Herstellung in winzigem Format denkbar. Ohne eigene Energieversorgung und nur kleiner Antenne, sind sie in kleinster Form denkbar. Solche Tags eigneten sich dementsprechend hervorragend, um sie in Alltagsgegenstände einzuarbeiten und nicht lediglich darauf zu applizieren. Der Vorteil liegt auf der Hand: Ein in ein T-Shirt eingearbeitetes Tag ist nicht sichtbar und selbst, wenn man von seiner Existenz wüsste, könnte man es nicht einfach entfernen ohne dabei Gefahr zu laufen, das Kleidungsstück zu beschädigen. Die Verhinderung einer solchen physischen Zerstörung oder Entfernung des Tags von dem Produkt stellt damit sicher, dass die RFID-Technik auch noch nach dem Kauf durch den Kunden eingesetzt werden kann, sodass der „elektronische Kassenzettel“ sowie neuartige Recycling-Maßnahmen möglich werden.

Die Speicherkapazität passiver RFID-Tags ist gering. Auf ihnen kann meist nur eine Identifikationsnummer aber keine weitergehenden Informationen gespeichert werden. Auch ein Wiederbeschreiben passiver Tags durch den Reader ist regelmäßig nicht möglich.

---

[15] Genaueres bei *Finkenzeller*, RFID-Handbuch, S. 23, 44, 55.

[16] *Heinrich* (Hrsg.), RFID and Beyond, macht auf S. 186 f. Ausführungen zur Preisentwicklung im Chip-Segment.

bb) Semi-aktive Tags

Die Besonderheit semi-aktiver Tags liegt darin, dass sie zwar eine eigene Energiequelle in Form einer Batterie haben, sie aber dennoch das durch den Reader erzeugte Energiefeld für die Kommunikation mit dem Reader nutzen.[17] Größe und Aufbau betreffend sind sie daher mit aktiven Tags vergleichbar, hinsichtlich der Sendereichweiten hingegen mit passiven. Eingesetzt werden solche semi-aktiven Tags beispielsweise bei elektronischen Mautsystemen wie *E-ZPass*. [18] Das hier verwendete Tag ist so groß wie ein Taschenbuch und verfügt über eine 5-Jahres-Batterie.

cc) Aktive Tags

Aktive RFID-Tags sind mit einer eigenen Energiequelle, meist einer Batterie, ausgestattet, die für die Energieversorgung des Mikrochips zuständig ist.[19] Dies führt dazu, dass sie wesentlich viel größer sind, teurer in der Herstellung und eine geringere Lebensdauer aufweisen als passive Tags, die immer wieder von Readern aktiviert werden können. Dafür haben sie zumeist aber auch eine sehr viel größere Sendereichweite (3 bis mehr als 100 Meter[20]), weil sie zur Aktivierung nicht auf die Energie des vom Reader generierten Feldes angewiesen, sondern schwächere Signale für die Kommunikation zwischen Tag und Reader ausreichend sind. Zudem lohnt sich bei aktiven Tags eher die Ausstattung mit einer größeren Speichereinheit. Aktive Tags können damit in der Regel mehr Daten selbstständig weiter senden. Sie sind daher auch keine „echten“ RFID-Transponder sondern vergleichbar mit Kurzstreckenfunkgeräten, auch *Short Range Devices* (SRD) genannt.[21] Zusätzlich ist bei aktiven Tags eine Wiederbeschreibfunktion denkbar. Daten könnten damit vom Reader gelöscht, verändert oder es können weitere Daten auf dem Tag gespeichert werden. Für den flächendeckenden Einsatz – beispielsweise dem Taggen von Einzelhandelsprodukten, bei dem es hauptsächlich darauf ankommt, die Kosten gering zu halten – scheiden aktive Tags damit aus. Anwendungsfelder ergeben sich allerdings in komplexeren Systemen, z.B. der Überwachung von Schiffscontainern. Hier sind die Kosten für ein energiebetriebenes RFID-Tag im Verhältnis zu anderen Technologien immer noch niedrig.

Einige aktive Tags können tausende Bytes Daten speichern. Solche Hochleistungs-Tags können beispielsweise in der Wartung und Reparatur von Maschinen Anwendung finden. Ein Mechaniker muss dann im Reparaturfall nicht in komplizierten Anleitungen nachsehen, welche Werkzeuge er benötigt. Er kann einfach das RFID-Tag mobilem Lesegerät auslesen und erhält umgehend die Informationen, die er für den Umgang mit der Maschine benötigt.[22]

---

[17] *Finkenzeller*, RFID-Handbuch, S. 24.

[18] *Garfinkel/Holtzman*, Understanding RFID Technology *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 18.

[19] *Finkenzeller*, RFID-Handbuch, S. 23.

[20] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 168.

[21] *Finkenzeller*, RFID-Handbuch, S. 25.

[22] *Heinrich* (Hrsg.), RFID and Beyond, S. 75.

dd) Speicherstruktur

In unterschiedlichsten Anwendungsbereichen müssen RFID-Systeme unterschiedlichsten Anforderungen gerecht werden. Je nach Anwendungsfeld ist dann entweder auf aktive, semi-aktive oder passive Tags zurückzugreifen. Wesentlich kommt es neben der Sendereichweite auch auf die Möglichkeit des Wiederbeschreibens des Tags und dessen Speicherstruktur an.[23] EPCglobal – das führende Unternehmen bei der Entwicklung des Industriestandards für den Electronic Product Code (EPC)[24] – hat eine Klassifizierung der RFID-Tags in sechs Klassen vorgenommen.[25]

<table>
<tr><td>(0) „Read only“</td><td>Passive Tags sind vom Hersteller programmiert und enthalten in der Regel nur eine Identifikationsnummer. Diese passiven Tags können nur noch ausgelesen werden.</td></tr>
<tr><td>(1) „Write once, read many times”</td><td>Passive Tags können auch erst vom Verwender nach dessen Anforderungen programmiert werden. Danach können auch diese Tags nur noch ausgelesen und nicht mehr wiederbeschrieben werden.</td></tr>
<tr><td>(2) „Read/Write“</td><td>Hier handelt es sich um wiederbeschreibbare passive Tags.</td></tr>
<tr><td>(3) Semi-aktive bzw. semi-passive Tags</td><td rowspan="3">Diese Tags können hingegen immer wieder neu programmiert, also die auf ihnen gespeicherten Daten verändert, gelöscht oder ergänzt werden.</td></tr>
<tr><td>(4) Aktive Tags</td></tr>
<tr><td>(5) Reader</td></tr>
</table>

Diese sechs Gruppen lassen sich vereinfacht auf drei reduzieren. Unterscheiden lassen sich nach der Speicherstruktur folgende Typen[26]:

(1) *Tags, die lediglich eine einzigartige Identifikationsnummer besitzen.* Diese Nummer kann entweder vom Hersteller oder erst vom Verwender programmiert werden. Es handelt sich hierbei um passive Tags, die günstig in der Herstellung sind und die großflächig eingesetzt werden sollen. Über die Verknüpfung mit einem Hintergrundsystem lassen sich dann weitere Daten abrufen. In Anwendungsbereichen, in denen das Tag nur eine Identifikationsnummer speichern muss, reichen Tags der Klassen (0) und (1) aus. Ist eine Wiederbeschreibbarkeit gewünscht, etwa um ein Tag wiederverwenden zu können, kommen auch Tags der Klasse (2) in Betracht.

(2) *Tags, die neben der einzigartigen Identifikationsnummer noch einen zusätzlichen Speicher für weitere Informationen aufweisen.* Eingesetzt werden hier (semi-)aktive Tags, so-

[23] Vgl. zu den verschiedenen denkbaren Speicherarchitekturen *Finkenzeller*, RFID-Handbuch, S. 324 ff., und zu den unterschiedlichen Speichertechnologien *ebd*., S. 343 ff.

[24] Hierzu unten mehr, Teil C.I.1.

[25] Vgl. *Garfinkel/Holtzman*, Understanding RFID Technology *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 19.

[26] Vgl. *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 81.

dass der Speicher sowohl ausgelesen als auch wiederbeschrieben werden kann. Solche Tags können sinnvollerweise dort eingesetzt werden, wo eine zeitnahe Verknüpfung mit einem Hintergrundsystem nicht möglich ist, wichtige Informationen aber dennoch sofort verfügbar sein sollen. In Betracht kommen hier demnach hauptsächlich Tags der Klassen (3) und (4).

(3) *Tags mit komplexer Speicherstruktur.* Sollen Tags nicht nur Informationen wiedergeben sondern möglicherweise selbstständig solche generieren, bedarf es neben einem größeren Speicher auch einer entsprechend leistungsfähigen Prozessoreinheit, die die Daten erstellt und verarbeitet. Solche Tags können beispielsweise mit Sensoren ausgestattet werden, die Daten sammeln. Auch in diesen Bereichen ist auf aktive Tags der Klasse (4) zurückzugreifen.

ee) Speicherkapazität

RFID-Tags können mit unterschiedlich großen Speichern ausgestattet werden. Die Größe des Speichers hängt davon ab, in welchem Bereich das Tag eingesetzt und wie viele Informationen darauf gespeichert werden sollen. Momentan variieren die Speicherkapazitäten von 32 Bits (das entspricht 4 Bytes) bis zu 32000 Bits (das entspricht 32 Kilobytes).[27] Es gilt allerdings die Regel, dass je weniger Informationen auf einem Tag gespeichert sind, desto weiter kann es vom Reader entfernt sein um trotzdem noch eine verlässliche Datenübertragung zu gewährleisten. Tags mit nur geringer Speicherkapazität können meist lediglich eine Identifikationsnummer und keine weiteren Informationen speichern. Solche preisgünstigen *read-only* Tags sollen nach Planung des AutoID-Teams – eine Gruppe Wissenschaftler, die gemeinsam mit EPCglobal die Entwicklung des *Internet of Things* vorantreiben[28] – in der Zukunft den Barcode auf Produktebene ersetzen.

Selbst bei einer Speichergröße von nur 80 Bits kann schon eine Nummer von 0 bis 1,2 x 1024 auf dem Tag gespeichert werden. Dies reichte aus, um einer riesigen Menge von Produkten eine einzigartige Identifikationsnummer zu verleihen. Zwar können außer einer eindeutigen Identifikationsnummer auf diesen Tags keine weiteren Informationen gespeichert werden, für die geplanten Zwecke ist dies aber auch völlig ausreichend. Tags mit einer Speicherkapazität von 32000 Bits können bereits bis zu elf Seiten Standard-Text mit doppeltem Zeilenabstand aufnehmen.[29] Dies reicht beispielsweise für ganze Wartungsanleitungen oder ähnliches.

ff) Sensor-Tags

In vielen Anwendungsfällen bietet es sich an, RFID-Tags zusätzlich mit Sensoren auszustatten, die beispielsweise Temperatur, Luftdruck oder Feuchtigkeit messen können.[30] Aufgrund des erhöhten Energiebedarfs solcher Sensor-Tags ist in den meisten Fällen auf aktive Tags

---

[27] *Heinrich* (Hrsg.), RFID and Beyond, S. 83.

[28] Hierzu unten mehr, Teil C.I.1.

[29] Für den gesamten Absatz vgl. *Heinrich* (Hrsg.), RFID and Beyond, S. 83.

[30] Vgl. *Finkenzeller*, RFID-Handbuch, S. 348 ff.

zurückzugreifen. Mit solchen Tags versehene Schiffscontainer können dann warnen, wenn die Feuchtigkeit für die empfindliche Fracht zu hoch ansteigt. In Maschinenteile implementierte Sensor-Tags können Aufschluss über die Wartungsbedürftigkeit geben, indem sie mittels der erfassten Druck- und Temperaturwerte auf die Abnutzung des Teils schließen lassen. In Kühllieferketten (z.B. bei Blutkonserven) kann mittels Temperatur messender Sensor-Tags nachvollzogen werden, ob die Güter zu hohen Temperaturen ausgesetzt waren und dementsprechend nicht mehr in den Handel gelangen bzw. verwendet werden dürfen. Sensor-Tags werden bei großer Leistungsfähigkeit und Komplexität auch als *Software-Agents* bezeichnet. Diese zeichnen sich dadurch aus, dass sie – je nach Ausstattung – unabhängig von einem IT-System selbstständig vorgegebene Prozesse ausführen und auf Umweltbegebenheiten reagieren.[31]

b) RFID Lese- bzw. Schreibgerät – „Reader“

Das Lesegerät – der "Reader" – sendet, sobald er eingeschaltet ist, unaufhörlich Radio-Wellen in der Erwartung, damit ein RFID-Tag zu erreichen und – wenn nötig – zu aktivieren. Wenn die vom Reader emittierten Wellen auf ein Tag treffen, wird dieses – sofern Reader und Tag kompatibel sind – aktiviert und sendet die auf ihm gespeicherten Informationen an den Reader. Bei aktiven Tags muss nicht einmal die Aktivierung erfolgen. Das aktive Tag sendet seine Daten dauernd an alle Reader in Reichweite.

Der Reader ist über eine serielle Schnittstelle oder eine Netzwerkverbindung mit einem Hintergrundsystem verbunden. Dieses Hintergrundsystem gibt die vom Nutzer programmierten Befehle an den Reader weiter. Je nach Befehl funkt der Reader dann ein in der Nähe befindliches Tag an und lässt sich von diesem die auf ihm gespeicherten Informationen senden oder aber er nimmt selbst Datenveränderungen auf dem Tag vor.[32] Die Daten, die der Reader empfängt, leitet dieser sodann weiter an das mit ihm verbundene IT-System.

Reader können ebenso wie Tags in verschiedenen Größen und Erscheinungsformen hergestellt werden.[33] Insbesondere im Logistik- und Lagerbereich kommen *Gate-Reader*, also „Tor“-Lesegeräte oder „Leseschleusen“, zum Einsatz. Hier werden mehrere Reader-Antennen auf einen mobilen Bogen oder statisch in Türrahmen installiert, durch die ganze Palletten oder Einkaufswagen hindurch geschoben werden können. Mittels Pulkerfassung lassen sich dann innerhalb kürzester Zeit alle Produkte identifizieren.[34] Insbesondere bei der Inventur auf der Verkaufsfläche bieten sich mobile Lesegeräte, sogenannte *Handheld-Reader* an. Diese mobilen Geräte können die gewonnenen Daten mittels WLAN direkt an das IT-System weitergeben oder aber zunächst speichern und später über eine Dockingstation weitergeben.

---

[31] Vgl. zu Software-Agents *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 137 ff.

[32] *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 70.

[33] Vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 169 f.

[34] Unter guten Bedingungen dürfte die maximale Tag-Identifikationsrate bei ca. 100 Tags in der Sekunde liegen, vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 171.

In diesem mobilen Bereich sind insbesondere auch RFID fähige Mobiltelefone, so genannte „NFC“ (*Near-Field-Communication*)-Handys, zu nennen. Nokia hat bereits vor Jahren begonnen RFID Technik in seine Mobiltelefone einzubauen bzw. entsprechende Adapter zu entwickeln.[35] In der Smartphone-Sparte hat Samsung gemeinsam mit Google begonnen, NFC-Technik in seine Nexus-Serie einzubauen.[36] Die Handys können sowohl als Tags als auch als Reader benutzt werden. Die Reader-Funktion kann von den Besitzern genutzt werden, um auf RFID-Tags gespeicherte Informationen – beispielsweise an Bushaltestellen oder Sehenswürdigkeiten – auszulesen.[37] Durch das Scannen dieser an bestimmten Stellen installierten Tags können entweder direkt weiterführende Informationen auf dem Handy sichtbar gemacht oder über den Handybrowser automatisch eine Verbindung zu einer entsprechenden Internetseite hergestellt werden. Mittels der Tag-Funktion können die Handys beispielsweise als E-Tickets im Personennahverkehr genutzt werden.

aa) Frequenzen

Wesentlicher Aspekt bei der Datenübertragung ist die Frequenz der Radiowellen.[38] Radiowellen haben bei verschiedenen Frequenzen sehr unterschiedliche Eigenschaften. Wellen in niedrigen Frequenzbereichen haben eine wesentlich geringere Reichweite als solche in hohen oder ultrahohen Frequenzbereichen. In den Niedrigfrequenzbereichen (LF und HF) wird für Energie- und Datentransfer das vom Reader generierte elektromagnetische Feld genutzt. Dieses erzielt keine mit elektromagnetischen Wellen vergleichbaren Distanzen. Daher muss sich das Tag im so genannten *Near-Field*-Bereich befinden, um effektiv mit ihm kommunizieren zu können. In höheren Frequenzbereichen (UHF und MW) hingegen findet der Energie- und Datentransfer mittels elektromagnetischer Wellen statt. Die hierdurch erzielten Sendereichweiten ermöglichen ein Auslesen der Tags auch aus größerer Distanz.[39] Solche Systeme werden deshalb auch als *Long-Range*-Systeme bezeichnet.[40] Niedrige Frequenzen können allerdings verschiedene Materialien besser durchdringen und sind damit vielfältiger einsetzbar.[41] Die Kehrseite ist, dass Wellen in niedrigen Frequenzbereichen weniger Daten in der Sekunde transportieren können als Wellen in höheren Frequenzbereichen. Für Anwendungen, bei denen "intelligentere" Chips mit größerer Speicherkapazität und eigener Rechenleistung benötigt werden, muss, um diese Vorteile auch nutzen zu können, auf hohe Frequenzen zurückge-

---

[35] Heise News Meldung vom 02.11.2004, Nokia stellt RFID-Handy-Hülle vor und testet Ticket-Verkauf, abrufbar unter http://www.heise.de/newsticker/meldung/Nokia-stellt-RFID-Handy-Huelle-vor-und-testet-Ticket-Verkauf-112574.html (04.04.2013).

[36] Heise News Meldung vom 19.10.2011, Galaxy Nexus: Google-Handy mit HD-Display und Android 4.0, abrufbar unter http://www.heise.de/mobil/meldung/Galaxy-Nexus-Google-Handy-mit-HD-Display-und-Android-4-0-1363207.html (04.04.2013); mehr unten Teil B.I.2.b)dd).

[37] *Heinrich* (Hrsg.), RFID and Beyond, S. 73, 75, 180; *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 159, mit weiteren Pilotprojekten auf S. 199 ff.

[38] Vgl. hierzu *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 73 ff.

[39] Vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 166 f.

[40] *Finkenzeller*, RFID-Handbuch, S. 50.

[41] *Finkenzeller*, RFID-Handbuch, S. 28.

griffen werden. Die Bedeutung der Frequenzhöhe ist vergleichbar mit der Taktung des Prozessors in einem PC: Je schneller der Prozessor ist, desto mehr Daten kann er in einer Zeiteinheit verarbeiten. Ebenso verhält es sich bei RFID-Tags: Je höher die Frequenz ist, auf der sie senden, desto mehr Daten können verarbeitet und gesendet werden.[42] In entsprechend hohen Frequenzbereichen ist eine Erfassung von bis zu 200 Tags in der Sekunde möglich.[43] Es wird unterschieden zwischen Niederfrequenzen (LF 100-135 kHz), Hochfrequenzen (HF 13,56 MHz), Ultrahochfrequenzen (UHF Europa 868 MHz, USA 915, Japan geplant 950-956 MHz) und Mikrowellen (MW 2,4 GHz und 5,8 GHz).[44] In Europa werden die Frequenzen im Bereich von 865 bis 868 MHz für *Short Range Devices*[45] verwendet.[46] Die Mikrowellen bieten den größtmöglichen Datentransfer und die schnellste Prozessortaktung. Mikrowellengestützte RFID-Tags können komplexe Rechnungen vornehmen und bei Anwendungen mit erhöhtem Gefahrenpotenzial eingesetzt werden. Aufgrund des kurzen Sendevorgangs können Mikrowellen besonders gut in Bereichen eingesetzt werden, in denen Tag und Reader sehr schnell aneinander vorbeigeführt werden. Der Nachteil der ultrahohen Frequenzen ist demgegenüber, dass die Radiowellen bestimmte Materialien nicht so gut durchdringen können wie Wellen in niederen Frequenzbereichen. Zu den am intensivsten genutzten Frequenzen gehören die im 13,56 MHz- sowie 2,45 GHz-Bereich.[47]

Nicht nur um Kollisionen mit bzw. Beeinträchtigungen anderer funkfrequenzgestützter Systeme[48] zu verhindern (Rundfunk, Polizei-, Schiffs- und Flugfunkdienste)[49] sondern insbesondere auch, um eine globale Kompatibilität verschiedenster RFID Systeme zu erreichen, ist neben der Harmonisierung der Komponenten auch die Standardisierung der verwendeten Frequenzen nötig. Eine barrierefreie Datenübertragung zwischen Komponenten verschiedener Systeme kann nur funktionieren, wenn der Übertragungsweg vereinheitlicht ist. Die Hersteller und insbesondere EPCglobal aber auch die zwischenstaatliche Organisation ITU (*Internatio-*

---

[42] *Heinrich* (Hrsg.), RFID and Beyond, S. 79.

[43] Deutscher Bundestag, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie, BTDrucks 16/7891 vom 23.01.2008, abrufbar unter http://dip21.bundestag.de/dip21/btd/16/078/1607891.pdf (04.04.2013), S. 4.

[44] *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 73; für China, Südafrika und Australien vgl. auch *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 105.

[45] Hierzu gehören neben RFID-Systemen auch noch eine Vielzahl anderer Anwendungen wie Modellfernsteuerungen, Garagentoröffner, Zentralverriegelungen, Außenthermometer, Bewegungsmelder, Geräte zum Auffinden von Lawinenverschütteten, Funkanlagen kleiner Leistung für medizinische Implantate, Warensicherungen, Bluetooth, Fahrzeugidentifikation für Schienenfahrzeuge, Verkehrstelematik und Abstandswarngeräte, Funkbewegungsmelder, Alarmfunkanlagen, induktive Funkanwendungen, drahtlose Mikrofone, WLAN u.a., *Finkenzeller*, RFID-Handbuch, S. 170.

[46] *Finkenzeller*, RFID-Handbuch, S. 171.

[47] *Finkenzeller*, RFID-Handbuch, S. 170, vermutet, dass dies der Fall ist, weil bei Einführung der ersten RFID-Systeme diese Frequenzbereiche weltweit gerade am häufigsten verfügbar waren, auch S. 174.

[48] Vgl. zu den verschiedenen Anwendungen in den unterschiedlichen Frequenzbereichen *Finkenzeller*, RFID-Handbuch, S. 169 ff., der auch darlegt, welche der angesprochenen Frequenzbereiche überhaupt für RFID-Systeme in Betracht kommen.

[49] *Finkenzeller*, RFID-Handbuch, S. 169.

nal Telecommunication Union)[50] wirken hier auf die Schaffung von Standards sowie die sinnvolle Verteilung der Frequenzen hin. In Europa wird die nationalstaatliche Regulierung mehr und mehr durch gemeinschaftliche Regulierung abgelöst, die von der *European Conference of Postal and Telecommunications Administrations* (CEPT) vorangetrieben wird.[51] In Deutschland ist für die Zulassung von RFID-Systemen die Bundesnetzagentur zuständig.[52] Allerdings liegen die meisten von RFID-Anwendungen genutzten Sendefrequenzen in den lizenzfreien ISM-Bändern (ISM = *Industrial-Scientific-Medical*), die für industrielle, wissenschaftliche und medizinische Anwendungen zur Verfügung stehen.[53] ISO-Normen spielen eine große Rolle bei der Standardisierung.[54] Die Bundesnetzagentur hat eine Übersicht veröffentlicht, in der RFID-Systeme mit verschiedenen Frequenznutzungen gegenüber gestellt werden.

RFID-Typ	Niederfrequenz	Hochfrequenz	Ultra-Hochfrequenz (UHF)	Mikrowelle
Arbeitsfrequenzbereiche	100 – 135 kHz	6,78 MHz 13,56 MHz 27,125 MHz	433,92 MHz 865 MHz (EU) 915 MHz (USA)	2,45 GHz, 5,8 GHz (in Vorbereitung)
Typische Lesereichweiten	einige mm bis 1 m	bis 3 m	bis 9 m	
Art der Kopplung von Leser und Transponder	induktiv	induktiv	elektromagnetisch	elektromagnetisch
Lesegeschwindigkeit	langsam	langsam bis mittel	schnell	sehr schnell
Anwendungsbeispiele	Tier-Identifizierung	Zugangskontrolle	Lager, Logistik	Fahrzeugidentifikation

Frequenzbereiche von RFID und ihre Parameter (Quelle: Bundesnetzagentur[55])

EPCglobal konzentriert sich maßgeblich auf passive UHF Tags (860-960 MHz), die über mehrere Meter ausgelesen werden können.[56] Dies ist zur automatischen Warenerkennung insbesondere im Bereich der Lagerlogistik erforderlich. UHF Tags sind allerdings für *Near-Field*-Anwendungen nicht geeignet. Insofern kommen eher HF Tags im Bereich von 13,56 MHz in Betracht. Es ist daher anzunehmen, dass beide Frequenzstandards parallel Verwendung finden werden. Zugangskarten bzw. -Token, elektronische Wegfahrsperren und implantierbare RFID-Tags (VeriChip) verwenden in der Regel Frequenzen im niedrigen Bereich. In der Medikamenten-Identifikation hat die U.S. amerikanische Food and Drug Administration

[50] Näheres bei Finkenzeller *Finkenzeller*, RFID-Handbuch, S. 180, vgl. auch die offizielle Homepage von ITU, http://www.itu.int/net/home/index.aspx (04.04.2013) und deren speziellen Bereich für Radiokommunikation http://www.itu.int/ITU-R/index.asp?category=information&rlink=rhome&lang=en (04.04.2013).

[51] *Finkenzeller*, RFID-Handbuch, S. 181 f., vgl. auch die offizielle Homepage von CEPT http://www.cept.org/ (04.04.2013); zur Frequenzverwaltung vgl. auch *Huber*, MMR, 2006, 728 (732).

[52] Vgl. hierzu *Finkenzeller*, RFID-Handbuch, S. 191 ff.

[53] Bundesnetzagentur, Informationsblatt „RFID, das kontaktlose Informationssystem“, abrufbar unter http://emf2.bundesnetzagentur.de/pdf/RFID-BNetzA.pdf (04.04.2013), S. 3.

[54] Bsp.: ISO 14443 (kontaktlose Chipkarten), ISO 15593 (Smart-Label und kontaktlose Chipkarten),vgl. bei *Finkenzeller*, RFID-Handbuch, S. 22.

[55] Bundesnetzagentur, Informationsblatt „RFID, das kontaktlose Informationssystem“, oben Fn. 53, S. 5.

[56] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 105.

(FDA) Frequenzen im Hochfrequenzbereich vorgeschrieben und die Produktidentifikation mittels EPC-basierter RFID Technik funktioniert über Hoch- und Ultrahochfrequenzen.[57]

bb) Lesereichweiten

Eins der wesentlichen Kriterien bei der Wahl des richtigen RFID Systems ist die Lesereichweite, die der eingesetzte Reader und die verwendeten Tags miteinander erreichen können. Es können hierbei drei verschiedene Klassen unterschieden werden:[58]

- *Close-Coupling-Systeme*, die lediglich eine Reichweite von bis zu einem Zentimeter haben,[59]
- *Remote-Coupling-Systeme*, die eine Sendereichweite von bis zu einem Meter erreichen und
- *Long-Range-Systeme*, die Sendereichweiten von über einem Meter aufweisen.

Close-Coupling-Systeme werden vor allem in sicherheitsrelevanten Bereichen, wie bei Zugangskontroll- oder Bezahlsystemen verwendet. Aufgrund der sehr geringen Lesereichweite müssen die getaggten Gegenstände (meist Chipkarten oder Token) in einen Kartenleser eingeführt oder direkt auf den Reader aufgelegt werden (*„touch&go"*).[60] *Remote-Coupling*-Systeme arbeiten regelmäßig mit niedrigen Frequenzen von 135 kHz oder 13,56 MHz. Long-Range-Systeme arbeiten typischerweise mit Sendefrequenzen von 868 bzw. 915 MHz oder aber 2,5 GHz.[61] Die maximal zu erreichende Sendereichweite hängt von verschiedenen Faktoren ab, wie der Sendefrequenz des Readers, Beschaffenheit der Antenne des Tags, Sendeleistung und Sensitivität des Readers aber auch den Umgebungsbedingen.[62] Die unter Idealbedingungen erreichte maximale Reichweite lässt sich deshalb unter normalen Alltagsbedingungen kaum verwirklichen und kann daher nur als Orientierungshilfe für den Vergleich verschiedener RFID-Systeme dienen. Unter idealen Bedingungen lassen sich für passive Tags Reichweiten bis maximal fünfzehn Metern[63], für aktive Tags Reichweiten bis zu 100 Metern erreichen[64].[65]

---

[57] Vgl. *Garfinkel/Holtzman*, Understanding RFID Technology *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 21.

[58] Vgl. hierzu *Finkenzeller*, RFID-Handbuch, S. 13; *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 77 f.

[59] *Finkenzeller*, RFID-Handbuch, S. 53.

[60] *Finkenzeller*, RFID-Handbuch, S. 53.

[61] *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 78.

[62] *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 78.

[63] *Finkenzeller*, RFID-Handbuch, 25.

[64] *Lampe/Flörkemeier/Haller*, Einführung in die RFID-Technologie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 76.

[65] Vgl. auch die Tabelle der Bundesnetzagentur oben.

cc) Kommunikation zwischen Reader und Tag

Die Kommunikation zwischen Reader und Tag funktioniert über das vom Reader generierte elektromagnetische Feld. Um eine weltweite Lesbarkeit der Tags zu garantieren, ist es erforderlich, dass die Luftschnittstelle – also das elektromagnetische Feld und entsprechend die verwendeten Frequenzen – standardisiert sind. Wie bereits gesehen, ist ein globaler Standard im 860-960 MHz Bereich wegen der Verwendung unterschiedlichster Frequenzen in verschiedenen Ländern nicht möglich. Um dennoch eine weltweite Kommunikationsfähigkeit der Tags zu ermöglichen, wäre es erforderlich, dass Tags im gesamten 860-960 MHz Bereich funktionierten. Dies würde die Herstellungskosten enorm in die Höhe treiben.[66] Aufgrund dieser Schwierigkeiten ist es nicht zu erwarten, dass sich ein globaler Standard wie eines *Internet of Things*[67] in naher Zukunft durchsetzt. Vielmehr wird es mittelfristig wahrscheinlich zu regional begrenzten Standards kommen, die sich aber bereits auf eine Vielzahl von Ländern erstrecken können wie das Beispiel der EU deutlich macht.

Für eine reibungslose Kommunikation zwischen Tag und Reader und damit der Erreichung einer maximalen Leseverlässlichkeit kommt es allerdings nicht nur auf die verwendeten Frequenzen an. Die Kommunikation durch die Luft ist anfälliger für äußere Einflüsse als Kommunikation mittels visuellen oder sonstigen physischen Kontakts. Nicht nur einige Materialien wirken sich nachteilig auf die Luftschnittstelle aus, sondern auch die räumliche Beziehung zwischen Tag und Reader. In bestimmten Winkeln ist ein Auslesen insbesondere mehrerer Tags auf einmal schwierig bis unmöglich.

dd) NFC – Near-Field-Communication

Near-Field-Communication beschreibt den Kommunikationsvorgang zwischen einem Tag und einem Reader im 13,56 MHz Frequenzbereich. Diese niedrige Frequenz lässt ein Auslesen des Tags nur bis zu wenigen Zentimetern zu und schafft damit eine vergleichsweise große Sicherheit vor unbefugtem Auslesen. Es verwundert daher nicht, dass sich unter den Mitgliedern des 2004 gegründeten „NFC Forums“[68] auch mehrere Kreditkartenunternehmen (so zumindest American Express, Master Card und Visa) wiederfinden. Wofür NFC in Zukunft genutzt werden soll, liegt damit auf der Hand. Bezahlvorgänge, die heute mittels des Magnetstreifens auf der Kreditkarte abgewickelt werden, könnten in Zukunft entweder über eine entsprechende Kreditkartenfunktion im NFC-Handy oder aber über die NFC-Kreditkarte selbst stattfinden.[69] Heute wird NFC-Technik bereits in *SmartCards* und dem elektronischen Reise-

[66] Vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 173.

[67] Hierzu unten mehr Teil C.I.1.

[68] www.nfc-forum.org (04.04.2013).

[69] Vgl. Heise News Meldung vom 23.11.2007, Master Card bringt drahtloses Bezahlen nach Deutschland, abrufbar unter http://www.heise.de/newsticker/meldung/Mastercard-bringt-drahtloses-Bezahlen-nach-Deutschland-Update-198726.html (04.04.2013) sowie Heise News Meldung vom 24.11.2006, Berührungsloses Zahlen mit Visa ab 2007 auch in Europa, abrufbar unter http://www.heise.de/newsticker/meldung/Beruehrungsloses-Zahlen-mit-Visa-ab-2007-auch-in-Europa-120901.html (04.04.2013).

pass sowie Personalausweis verwendet.[70] Nachdem die Debatte über NFC zwischenzeitlich deutlich ruhiger geworden war, hat jetzt einer der *Major Player* im Internetgeschäft einen neuen erfolgsversprechenden Vorstoß gewagt: Google hat in sein jüngst vorgestelltes Google-Mobiltelefon der zweiten Generation, dem Nexus S, hergestellt von Samsung, einen NFC-Chip integriert.[71] Mit diesem sollen Bezahlvorgänge über das Handy abgewickelt werden können. Künftig sollen auch andere Handys mittels NFC-fähiger MicroSD-Karte nachgerüstet werden können.[72] Erste Finanzinstitute – Master Card und die Citygroup – gehören offenbar schon zu Googles neuen Partnern.[73]

c) RFID Hintergrundsystem – „Backend"

Die vom Reader empfangenen Daten sind ohne weitere Verarbeitung in vielen Fällen nutzlos. Sie müssen organisiert werden. Dies geschieht mittels des mit dem Reader verbundenen im Hintergrund agierenden IT-Systems, dem sog. „Backend". Von diesem gehen zunächst die Befehle an den Reader aus: Soll er lediglich Daten auslesen, soll er löschen oder verändern. Kommen dann Daten vom Reader zurück an das IT-System, werden diese verarbeitet: Sollen sie lediglich gespeichert oder auch organisiert werden oder sollen sie einen bestimmten Prozess initiieren, wie das Öffnen einer Tür.

Hinsichtlich der Kommunikation zwischen dem Lesegerät und dem Hintergrundsystem ergeben sich abhängig von der Beschaffenheit der Reader Unterschiede. Bei fest installierten Readern ist die Datenübertragung über Datenkabel oder WLAN möglich. Bei mobilen Lesegeräten hingegen scheidet eine Verkabelung in der Regel mangels Praktikabilität aus. Entsprechend ist die Verarbeitung der eingelesenen Daten entweder mittels eines Kombinationsgerätes möglich, das gleichzeitig Lesegerät und Computer ist, oder die Daten werden drahtlos mittels GSM, GPRS, UMTS oder Satellitenfunk (INMARSAT) an den Rechner, auf dem das Hintergrundsystem gespeichert ist, gesendet.[74]

aa) Software

Das Backend kann je nach Bedarf verschiedene Arbeitsschritte mit den eingelesenen Daten vornehmen.[75] Hierfür erforderlich ist entsprechende Software. Grundsätzlich durchlaufen die

---

[70] Vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 177.

[71] Heise News Meldung vom 19.10.2011, Galaxy Nexus: Google-Handy mit HD-Display und Android 4.0, abrufbar unter http://www.heise.de/mobil/meldung/Galaxy-Nexus-Google-Handy-mit-HD-Display-und-Android-4-0-1363207.html (04.04.2013).

[72] Heise News Meldung vom 15.11.2011, NFC-Nachrüstsatz für Handys, abrufbar unter http://www.heise.de/newsticker/meldung/NFC-Nachruestsatz-fuer-Handys-1379208.html (04.04.2013).

[73] The Wall Street Journal vom 28.03.2011, Google Sets Role in Mobile Payment, abrufbar unter http://online.wsj.com/article/SB10001424052748703576204576226722412152678.html?KEYWORDS=google+android (04.04.2013).

[74] BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, abrufbar unter http://www.bitkom.org/files/documents/White_Paper_RFID_deutsch_11.08.2005_final.pdf (04.04.2013), S. 12, 14, 26.

[75] Vgl. zu verschiedenen Systemarchitekturen BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 12.

Daten zwei Stufen: Die *Edgeware* und die *Middleware*. Die *Edgeware* bereinigt die gescannten Daten und filtert sie soweit, dass nur noch die für die *Middleware* wichtigen Daten weitergeleitet werden. Die *Middleware* bereitet dann die Daten für die vom Betreiber verwendeten Geschäftsapplikationen vor.

bb) Speicherung

Die mittels der *Middleware* gewonnenen und an die Anwendungssoftware weitergeleiteten Daten sind in vielen Fällen sinnvollerweise in Datenbanken zu speichern. RFID kann damit nicht nur *Real-time*-Vorteile erzielen, sondern auch für Langzeitbetrachtungen eingesetzt werden. Bestes Beispiel sind Tracking-Szenarien, in denen das Kundenverhalten analysiert wird.[76] Ohne die Speicherung der anonymen oder individualisierten Kundenbewegung und des Kundenverhaltens ist eine hierauf abgestimmte Anpassung der Verkaufsstrategien des Verkäufers undenkbar.

Unterscheiden lässt sich grundlegend zwischen *zentralem* und *dezentralem* Datenmanagement. Für die datenschutzrechtliche Bewertung kommt es unter anderem darauf an, ob auf dem Tag selbst (personenbezogene) Daten oder nur eine Identifikationsnummer gespeichert und die weitergehenden Informationen in einer Datenbank abgelegt sind. In einigen Anwendungen macht es durchaus Sinn, Tags mit größerem Speicher einzusetzen und direkt Daten auf diesem zu speichern, insbesondere dann, wenn ein Abruf der Information aus der Datenbank mangels Internetzugang nicht möglich ist. Für diese Arbeit entscheidend ist, dass es beide Formen gibt und für den Kunden oder sonst Betroffenen, der ein oder mehrere RFID-Tags bei sich führt, in den meisten Fällen nicht erkennbar ist, was genau auf dem Tag gespeichert ist.

II. RFID-Anwendungen

RFID findet bereits heute in diversen Bereichen Anwendung. Es ist zu erwarten, dass immer neue Anwendungsbereiche erschlossen werden, wo Identifikation eine Rolle spielt. Vollständigkeit kann diese Arbeit aufgrund der immer neuen und ständig zu erweiternden Einsatzgebiete nicht bieten.[77] Allerdings werden die wesentlichen und für die datenschutzrechtliche Debatte entscheidenden Bereiche vorgestellt.

1. Unterscheidung zwischen offenen und geschlossenen RFID-Systemen

Teilweise wird hierbei eine Unterteilung in offene und geschlossene RFID-Anwendungen vorgenommen[78]: Geschlossene Systeme zeichneten sich dadurch aus, dass aufgrund der tech-

[76] Hierzu unten mehr, C.II.

[77] Die Recherche zu RFID-Anwendungen fand größtenteils vor 2009 statt. Die aktuellen Entwicklungen wurden allerdings berücksichtigt, soweit sie für die Ergebnisse dieser Arbeit relevant waren. Eine Überarbeitung der diversen Einsatzfelder vor Veröffentlichung erschien nicht geboten, weil die Unterschiede zu den bereits bekannten Anwendungen regelmäßig gering waren – eine andere praktische oder rechtliche Betrachtung hätte sich entsprechend nicht ergeben.

[78] *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, abrufbar unter http://www.qucosa.de/fileadmin/data/qucosa/documents/5562/data/Dissertation.pdf (04.04.2013), S. 59; Bun-

nischen Parameter keine Kompatibilität mit Komponenten anderer Systeme besteht. Offene Systeme setzten hingegen auf Standards, sodass hier eine entsprechende Kompatibilität mit einer nicht überschaubaren Anzahl von Komponenten anderer Systeme erreicht werden könne. Hieraus ergäbe sich auch der Grund für die Unterteilung: In offenen und geschlossenen RFID-Anwendungen herrschten aufgrund der technischen Voraussetzungen unterschiedliche Gefahren für das allgemeine Persönlichkeitsrecht des Einzelnen.[79] So wird darauf verwiesen, dass in geschlossenen Anwendungen der Kreis der potenziell Betroffenen regelmäßig überschaubar bliebe, während in offenen Anwendungen eine unüberschaubare Vielzahl potenziell Betroffener berücksichtigt werden müsse.

Dieser Annahme ist zu widersprechen: In einer Welt ubiquitärer RFID-Anwendungen ist nicht auszuschließen, dass es immer wieder zu technischen Kompatibilitäten kommen kann, die dazu führen, dass Daten auch aus Tags, die für ein bestimmtes geschlossenes System bestimmt sind, ausgelesen werden können. Entsprechend müssen RFID-Systeme im Zweifel immer als offene Systeme betrachtet werden,[80] sodass eine Unterscheidung in dieser Arbeit entbehrlich ist. Jedenfalls auf dem Weg zu einem „Internet der Dinge“ ist die Offenheit der verwendeten Systeme unabdingbar, sodass in den meisten Bereichen auch mit den Meinungen, die Unterscheidungen vornehmen, hier eindeutig von einem offenen System auszugehen ist.[81]

2. Produktidentifikation in Handel und Anlagenverwaltung

Mit Hilfe von RFID sollen logistische Abläufe in der Herstellungs- und Lieferkette vereinfacht und fehlerunanfälliger gemacht werden.[82] Zwei wesentliche Ziele sind die Reduzierung von Beständen und damit die Reduzierung von Lager- und Kapitalbindungskosten sowie die Reduzierung von Personalkosten in den Geschäften und Lagern.[83] RFID getaggte Produkte können schnell am Waren-Ein- und Ausgang erfasst werden. Fehler bei der automatisierten

---

desministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, abrufbar unter http://www.bmbf.de/pubRD/ita_taucis.pdf (04.04.2013), S. 244.

[79] *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 248.

[80] Zu diesem Schluss kommt am Ende seiner Arbeit dann doch auch *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 283; vgl. auch Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 209 f.

[81] Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 245.

[82] Vgl. zu den logistischen Vorteilen, die RFID in der Produktions- und Lieferkette mit sich bringt bei *Heinrich* (Hrsg.), RFID and Beyond, S. 60 f; *Simchi-Levi*, The Impact of RFID on Supply Chain Efficiency *in*: Heinrich (Hrsg.), RFID and Beyond, S. 214 ff; *Tellkamp/Quide*, Einsatz von RFID in der Bekleidungsindustrie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 146 ff.; *Tellkamp/Haller*, Automatische Produktidentifikation in der Supply Chain des Einzelhandels *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 227 ff; von *Westerholt/Döring*, CR 2004, 710 f.

[83] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/RIKCHA_pdf.pdf?__blob=publicationFile (04.04.2013), S. 75.

Erfassung können im Vergleich zur manuellen vermieden werden. Die Lagerverwaltung kann mittels RFID-Tags an den Produkten und im Lager installierter Reader effektiver gestaltet werden, indem ausverkaufte Waren automatisch nachbestellt und falsch abgestellte Paletten schnell wiedergefunden werden.[84] Mittels *Smart Shelves* –Warenregalen mit Reader-Funktion – auf der Verkaufsfläche wird eine automatische Inventur möglich, ebenso, wie auch hier der Befehl zum Auffüllen leerer Regale automatisch an das System geschickt werden kann. Die heute flächendeckend zur Diebstahlsicherung eingesetzten 1-Bit-Transponder[85] können durch RFID-Tags eingespart werden, weil diese die Aufgabe einfach mit übernehmen könnten. Der Kassiervorgang kann beschleunigt werden, weil ein Finden und Einscannen des Barcodes an den Produkten überflüssig würde. Insbesondere bei wertvollen Artikeln oder Medikamenten könnte das RFID-Tag als Authentifizierungsmerkmal dienen und so Fälschungssicherheit gewähren.[86] Unter den Begriff Authentifizierung kann auch das Speichern von Kassenbelegen oder gar Garantien auf dem RFID-Tag oder im Hintergrundsystem gefasst werden.

Die aus Unternehmersicht bestehenden Vorzüge, die RFID gestützte Warenidentifikation mit sich bringen, sind natürlich nicht unbeachtet geblieben. Seit einiger Zeit führen diverse Unternehmen RFID-Technik ein. Beispielhaft genannt seien hier Benetton, METRO, Kaufhof mit GERRY WEBER, Karstadt und C&A. Bereits 2003 kündigte der weltweit operierende Textilhersteller Benetton an, Kleidungsstücke seiner Marke Sisley künftig mit RFID-Tags versehen zu wollen. Auf diese Neuigkeit reagierte die Öffentlichkeit allerdings derart entrüstet, dass das Unternehmen sich gezwungen sah, seine Pläne zurückzuziehen.[87]

Metro – Deutschlands größte Einzelhandelskette[88] – hat ebenfalls 2003 als eine Art Pionier-Unternehmen einen „*Future-Store*“[89] in Rheinberg eröffnet. In diesem als Pilotprojekt geführten Markt sind alle Artikel mit einem RFID-Tag und Warenregale und Einkaufswagen mit einem Reader versehen. Zusätzlich sind an den Einkaufswagen sowie im gesamten Markt Bildschirme installiert, die den Kunden Wareninformationen und Werbung präsentieren.[90]

---

[84] Mit einem derart „aufgerüsteten“ Einzelhandel ließe sich der „*Bullwhip*“-Effekt weitgehend vermeiden, vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 52 ff.

[85] 1-Bit-Transoponder genügen für die Diebstahlsicherung aus, weil die mit diesen mögliche Darstellung zweier Zustände ausreicht. Wird der Transponder an der Kasse nicht entfernt und begibt sich ein Kunde mit dem weiterhin getaggten Gegenstand durch die Leseschranke am Ausgang, sendet der Transponder sein Signal und das System erkennt „Transponder in Lesereichweite“ und entsprechend „Ware nicht bezahlt“ (natürlich kann es vorkommen, dass an der Kasse einmal ein Transponder übersehen und mithin nicht entfernt wird). Wurde der Transponder beim Bezahlen entfernt, kann das Signal auch nicht gesendet werden. Vgl. zu den 1-Bit-Transpondern *Finkenzeller*, RFID-Handbuch, S. 32.

[86] Zum Bedürfnis Fälschungssicherheit zu gewährleisten vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 25 ff.

[87] Vgl. die von CASPIAN ins Leben gerufene Website „Boycott Benetton“, http://www.boycottbenetton.com/ (04.04.2013). CASPIAN steht für „Consumers Against Supermarket Privacy Invasions And Numbering”, vgl. http://www.nocards.org/ (04.04.2013).

[88] *Heinrich* (Hrsg.), RFID and Beyond, S. 58.

[89] http://www.future-store.org/fsi-internet/html/de/375/index.html (04.04.2013).

[90] *Heinrich* (Hrsg.), RFID and Beyond, S. 59.

Ziel ist es, die Vorzüge der Technik zu erproben und die Kundenakzeptanz zu untersuchen.[91] Metro arbeitet mit verschiedenen Herstellerfirmen[92] zusammen, denen ebenfalls am Sammeln von RFID-Erfahrungen gelegen ist. Metro hat außerdem ebenfalls bereits 2003 angekündigt, ab 2005 ihre 100 Top-Zulieferer zu verpflichten, alle Palletten mit RIFD-Tags zu versehen.[93] Zurzeit versehen rund 180 Lieferanten ihre für die METRO GROUP bestimmten Paletten und Kartons mit RFID-Tags; den zugehörigen EPC – die eindeutige Identifikationsnummer – speichert METRO selbst auf dem Tag.[94]

Die GALERIA Kaufhof GmbH – ein Unternehmen der METRO GROUP – hat in einem Pilotprojekt mit GERRY WEBER dessen RFID getaggte Produkte in der Filiale Essen von September 2007 bis Dezember 2008 zum Verkauf bereitgehalten.[95] Weiterhin waren ein Logistikbetrieb sowie ein Kaufhof-Lager beteiligt. Überprüft werden sollte u.a., inwieweit der Wareneingang mittels RFID beschleunigt und fehlerunanfälliger gemacht werden kann.[96] Im Rahmen des Projekts wurden alle entsprechenden Kleidungsstücke manuell mit einem RFID-Tag versehen.

Auch Karstadt hat nach entsprechender Medienberichterstattung 2007 begonnen RFID getaggte Produkte in seinen Warenhäusern zu verkaufen.[97] Mehrere Hersteller hatten sich bereit erklärt ihre Artikel bereits vor Auslieferung an Karstadt mit den entsprechenden Tags zu versehen. Zum damaligen Zeitpunkt plante das Unternehmen noch eine vollständige Umrüstung innerhalb eines Jahres also bis Ende 2008 in allen Filialen. Neben der Einführung von RFID sollte gleichzeitig ein TV-System in den Häusern installiert werden mittels dessen kundensensitive Werbung geschaltet werden kann.[98]

Eines der jüngsten Beispiele für die Einführung von RFID auf Produktebene ist C&A. Das Unternehmen stattet seit Sommer 2012 zunehmend Produkte und Filialen mit RFID aus.[99]

---

[91] RFID Journal vom 28.03.2003, Metro Opens 'Store of the Future, abrufbar unter http://www.rfidjournal.com/article/articleview/399/1/1 (04.04.2013).

[92] Vgl. *Albrecht/McIntyre*, Spychips, S.71

[93] *Sarma*, A History of the EPC *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 53.

[94] Vgl. die Homepage des Metro Future Store, abrufbar unter http://future-store.org/fsi-internet/html/de/1564/index.html (04.04.2013).

[95] Vgl. die Homepage des Metro Future Store, abrufbar unter http://future-store.org/fsi-internet/html/de/1613/index.html (04.04.2013).

[96] *Tellkamp/Quide*, Einsatz von RFID in der Bekleidungsindustrie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, 150.

[97] Heise News Meldung vom 10.09.2007, Karstadt führt RFID-Etiketten ein, abrufbar unter http://www.heise.de/newsticker/meldung/95771 (04.04.2013).

[98] Dass diese Pläne zwischenzeitlich umgesetzt worden sind, konnte bis zur Veröffentlichung nicht nachvollzogen werden.

[99] Eine Liste der Filialen findet sich auf der Website von C&A, abrufbar unter http://www.c-and-a.com/de/de/corporate/fashion/wir-fuer-sie/informationen-zu-rfid/ (04.04.2013). Hier finden sich auch Kundeninformationen über RFID, so u.a. der Hinweis, dass die Tags unmittelbar nach dem Einkauf entfernt werden können.

Ziel ist es, das Angebot in den Filialen zu verbessern und insbesondere die Produkte in möglichst großer Farb- und Größenvielfalt vorrätig zu haben.[100]

Die wirtschaftlichen Vorteile von RFID können in mannigfaltiger Weise eingesetzt werden. NCR, eines der weltweit führenden Unternehmen für die Herstellung von Kassensystemen, hat bereits 2003 eine Broschüre herausgegeben, in der „50 Ideen" für die Verwendung von RFID in Geschäften dargestellt werden.[101] Im Folgenden werden einige dieser Praxisbeispiele den Bereichen Fälschungsschutz, Diebstahlsicherung, Anlagenverwaltung, Inventur, gesetzliche Pflichten, Bezahlvorgang, Reklamation und Rückgabe zugeordnet.

a) Fälschungsschutz

Insbesondere das Taggen von Medikamenten könnte mehr Sicherheit vor Fälschungen bieten. Es werden immer mehr Fälle von gefälschten Medikamenten bekannt.[102] Abgesehen von den wirtschaftlichen Schäden, die hierdurch jährlich entstehen, bergen gefälschte Medikamente insbesondere auch enorme Gefahren für die Gesundheit der Patienten. Ein RFID-Tag mit eindeutiger Identifikationsmöglichkeit auf jeder Packung könnte Fälschungssicherheit bieten. Bereits 2004 hat die U.S. amerikanische *Food and Drug Administration* (FDA) die Empfehlung ausgesprochen, bis 2007 alle auf dem amerikanischen Markt zu vertreibenden Medikamente mit RFID auszustatten.[103] Ziel dieser rechtlich nicht bindenden Empfehlung ist, eine lückenlose Rückverfolgbarkeit der Medikamente und damit größtmögliche Verbrauchersicherheit zu gewährleisten. Die zeitliche Vorgabe konnte von der Industrie jedoch nicht eingehalten werden.

Auf U.S. Bundesebene gibt es ein entsprechendes Gesetz, das die Etikettierung von Medikamenten mit einer standardisierten Identifikationsnummer vorschreibt.[104] Dort wird RFID als eine der möglichen Techniken zur Erreichung dieses Ziels aufgezählt.[105]

> U.S. Public Law 110-85, Sec. 505d "Pharmaceutical Security" Subsec. (b) (3)
>
> "(a) In General. – The Secretary shall develop standards and identify and validate effective technologies for the purpose of securing the drug supply chain against counterfeit, diverted, subpotent, substandard, adulterated, misbranded, or expired drugs.
>
> (b) Standards Development.--

---

[100] Dies teilte C&A 2012 in einer Pressemitteilung vom 01.06.2012 mit, abrufbar unter http://www.c-and-a.com/de/de/corporate/fileadmin/mediathek/de-de/Pressemitteilungen/C-und-A_startet_RFID-Projekt_an_f%C3%BCnf_Standorten.pdf (04.04.2013).

[101] Vgl. *Albrecht/McIntyre*, Spychips, S. 73.

[102] Nach Schätzungen der WHO stammen 4-8 % des weltweiten Umsatzes im Pharmabereich aus dem Verkauf von gefälschten Medikamenten, vgl. *Koh/Staake*, Nutzen von RFID zur Sicherung der Supply Chain der Pharmaindustrie *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 116 f.

[103] Die Empfehlung ist ausgesprochen worden in einem Report der FDA zur Bekämpfung gefälschter Medikamente: U.S. Food and Drug Administration, „Combating Counterfeit Drugs", 2004, http://www.fda.gov/Drugs/DrugSafety/ucm173297.htm (04.04.2013).

[104] Public Law 110-85, vom 27.09.2007, 121 Stat. 823, abrufbar unter http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ085.110.pdf (04.04.2013).

[105] Public Law 110-85, Sec. 505d "Pharmaceutical Security" Sub. Sec. (b) (3), vom 27.09.2007, 121 Stat. 823, oben Fn. 104.

> (1) In general. – The Secretary shall, in consultation with the agencies specified in paragraph (4), manufacturers, distributors, pharmacies, and other supply chain stakeholders, prioritize and develop standards for the identification, validation, authentication, and tracking and tracing of prescription drugs.
>
> (2) Standardized numeral identifier. –
>
> Not later than 30 months after the date of the enactment of the Food and Drug Administration Amendments Act of 2007, the Secretary shall develop a standardized numerical identifier (which, to the extent practicable, shall be harmonized with international consensus standards for such an identifier) to be applied to a prescription drug at the point of manufacturing and repackaging (in which case the numerical identifier shall be linked to the numerical identifier applied at the point of manufacturing) at the package or pallet level, sufficient to facilitate the identification, validation, authentication, and tracking and tracing of the prescription drug.
>
> (3) Promising technologies. – The standards developed under this subsection shall address promising technologies, which may include –
>
> (A) **radio frequency identification technology** [Hervorh. eingef. D. Verf.];
>
> (B) nanotechnology;
>
> (C) encryption technologies; and
>
> (D) other track-and-trace or authentication technologies.
>
> (…)"

Es gab noch eine weitere Gesetzesinitiative auf US-Bundesebene, mit der ebenfalls die Etikettierung von Medikamentenverpackungen mit RFID-Tags oder vergleichbaren Identifikationsmerkmalen verpflichtend werden sollte.[106] Das Gesetz ist aber nicht verabschiedet worden.

Auch Markenartikel können mit RFID fälschungssicherer gemacht werden. Im Luxusgüterbereich könnte dies den Einzelnen vor finanziellen Verlusten schützen. Aber auch im Massenproduktionsbereich wird RFID zur Vermeidung von Plagiarismus eingesetzt. So statten die Druckerhersteller Epson und Canon ihre Kartuschen für Tintenstrahldrucker mit RFID aus, um es der Konkurrenz zu erschweren, preisgünstigere Nachbildungen ihrer Produkte herzustellen.[107]

Im industriellen Bereich hingegen spielt Fälschungssicherheit insbesondere eine sicherheitstechnische Rolle. Mit RFID getaggten Bauteilen ließe sich beispielsweise in der Flugzeugindustrie und -wartung an Fälschungs- und gleichzeitig Passagiersicherheit gewinnen. Airbus plant vor diesem Hintergrund auch Ersatzteile für seinen neuen 787 Dreamliner mit passiven RFID-Tags auszustatten, um diese identifizieren zu können. Gleichzeitig sollen die mit einem Speicher ausgestatteten Tags die Wartungshistorie speichern können.[108] Auch Delta Air Lines hat bereits mit der Ausstattung von Flugzeugtriebwerken mit RFID und Sensoren begonnen, um so automatische Wartungen durchführen zu können.[109]

---

[106] H.R. 2716, 2007, „Reducing Fraudulent and Imitation Drugs Act of 2007", http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2716: (04.04.2013).

[107] *Scheuch*, Günstiger Drucker, teure Tinte, ZDFheute.de WISO Meldung vom 24.04.2006, abrufbar unter http://www.tintenfuzzy.de/Wissen/LinkedDocuments/wiso2.pdf (04.04.2013).

[108] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 115.

[109] *Heinrich* (Hrsg.), RFID and Beyond, S. 69, 141 ff., 179; vgl. zum Wartungsprozess auch Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 75.

b) Diebstahlsicherung

Die im Einzelhandel zur Diebstahlsicherung weit verbreitet eingesetzten 1-Bit-Transponder könnten möglicherweise durch RFID-Tags ersetzt werden. Das ohnehin am Produkt angebrachte Tag könnte diese Aufgabe mit übernehmen. Ein 1-Bit-Transponder ist im Grunde nichts anderes als ein sehr einfaches RFID-Tag. Im Unterschied zu diesen verfügt er allerdings über einen viel kleineren Speicher und kann deshalb auch nur ein Bit an Informationen übermitteln.

c) Anlagenverwaltung

Unter dem Stichwort Anlagenverwaltung wird hier der Einsatz von RFID in Bibliotheken, Gerichtsakten und der Luftfahrt gefasst.

In der Luftfahrt ist die Verwendung von RFID neben der oben bereits erwähnten Frage der Fälschungssicherheit beim Flugzeugbau und -wartung auch in der Anlagenverwaltung denkbar. Bauteile und Werkzeuge – mit RFID ausgestattet – können hinsichtlich ihrer Benutzungsdauer überwacht, auf ihre Echtheit überprüft und in der Wartungshalle wiedergefunden werden. Aber auch im Bereich der Gepäckabfertigung kann RFID als Ersatz für den bislang verwendeten Barcode eingesetzt werden.[110] Ebenso ist eine Verwendung von RFID im Passagier-Bereich, z.B. mittels getaggter Boardkarten[111], möglich.

RFID gestützte Systeme werden auch in der Justiz verwendet. In einem Pilotprojekt des Landgerichts Detmold werden Gerichtsakten mit einem RFID-Tag versehen. Damit soll die Registratur und insbesondere das Auffinden der Akten vereinfacht und automatisiert werden. Zudem wird eine Verbindung von papierner und elektronischer Akte hergestellt. So kann außerdem in Kombination mit einem speziellen Verwaltungsprogramm, mit dem beispielsweise Diktate erstellt werden können, die Arbeit der Serviceeinheiten erleichtert werden.[112]

In Bibliotheken bietet sich die Verwendung von RFID an.[113] Nicht nur das Wiederfinden von Büchern, auch der Ausleihvorgang kann damit automatisiert und somit effektiver gestaltet werden. Selbst der Vatikan hat seine Bibliothek mit RFID ausgerüstet.[114]

---

[110] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, abrufbar unter http://www.europarl.europa.eu/RegData/etudes/etudes/join/2007/383219/IPOL-JOIN_ET(2007)383219_EN.pdf (04.04.2013), S. 24; RFID Journal (Jonathan Collins), vom 18.08.2006, Air France-KLM Embarks on RFID Luggage-Tag Trial, abrufbar unter http://www.rfidjournal.com/article/articleview/2600/1/1 (04.04.2013); Interview mit Stefan Lauer, Vorstandsmitglied der Deutschen Lufthansa AG, *Heinrich* (Hrsg.), RFID and Beyond, S. 147 f.

[111] c't Magazin 23/06, Operation RFID-Tag startet in Ungarn, abrufbar unter http://www.heise.de/ct/artikel/Operation-RFID-Tag-startet-in-Ungarn-290732.html (04.04.2013).

[112] Das Landgericht Detmold arbeitet mit dem Programm „Findentity". Vgl. die Homepage des Herstellers THAX, abrufbar unter http://www.thax.de/ (04.04.2013); RFID Journal vom 30.04.2008, In German Courts, RFID Dictates Where Audio Files Are Stored, http://www.rfidjournal.com/article/articleview/4059/1/1/ (04.04.2013).

[113] Vgl. hierzu *Bowen*, Wireless Tracking in the Library: Benefits, Threats, and Responsibilities *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 229 ff.

[114] *Thiesse/Gillert*, Das smarte Buch *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 291-299.

d) Inventur

RFID kann, sowohl im Einzelhandel als auch in sicherheitsrelevanten Umgebungen wie Krankenhäusern, eine automatisierte Inventur ermöglichen und somit Zeit und Geld sparen helfen. Aber auch in anderen Bereichen, in denen die Optimierung logistischer Prozesse angestrebt wird und Inventuren zwangsläufig erforderlich sind, kann RFID Verbesserungen bringen.

Um das Inventurverfahren in Supermärkten oder sonstigen Einzelhandelsgeschäften möglichst reibungslos zu gestalten, müssen die Geschäftsräume entweder zeitweise für die Öffentlichkeit geschlossen werden oder aber die Angestellten müssen Nachtschichten einlegen. Dies kann mit RFID verhindert werden. *Smart Shelves*, also Warenregale mit eingebautem RFID Lesegerät, können kontinuierlich oder zu einem bestimmten Zeitpunkt alle in ihrer Nähe befindlichen Waren scannen. Alternativ und unter Vermeidung solcher *Smart Shelves* könnte das Personal auch mit mobilen Lesegeräten durch die Regale gehen und auf diesem Wege den Warenbestand überprüfen. Bei beiden Methoden wird viel Zeit gespart und somit auch hier eine Verbesserung des Geschäftsprozesses bewirkt.

Auch in hochsensiblen Bereichen wie Krankenhäusern bietet sich der Einsatz von RFID an.[115] Inventar und medizinische Instrumente können getaggt werden. Würde vor und nach jeder Operation ein Scanvorgang innerhalb des OPs durgeführt, ließe sich weitgehend verhindern, dass medizinische Geräte im Körper des Patienten vergessen werden.[116] Ebenso könnte mit einem mobilen Lesegerät der Körper des Patienten am Ende der OP „gescannt“ und vergessene Instrumente so gefunden werden. Auch künstlich hergestellte Implantate könnten mit RFID ausgerüstet werden. Ein komplexes Tag in Kombination mit einem Sensor könnte dann sogar Aufschluss über die Beschaffenheit des Implantates liefern. So ließen sich weitere Operationen für den Patienten ganz verhindern oder zumindest ihre Zahl reduzieren.

e) Gesetzliche Pflichten

Automatische Autorisierungsverfahren könnten Einzelhändlern die Einhaltung der ihnen gesetzlich obliegenden Pflichten erleichtern.[117] Beispielhaft sei hier der METRO Future Store genannt, der sich RFID unter anderem auch in der Film-Abteilung zu Nutzen macht. Um die Einhaltung der Jugendschutzvorschriften zu gewährleisten, muss ein Verkäufer grundsätzlich jeden Kunden, der einen nicht-jugendfreien Film kaufen oder nur probesehen möchte, nach seinem Alter fragen und den Kunden bitten, sich entsprechend auszuweisen. METRO hat diesen Vorgang automatisiert und das Probeschauen von Filmen davon abhängig gemacht, dass

[115] *Fishkin/Lundell*, RFID in Healthcare *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 211ff.

[116] *Heinrich* (Hrsg.), RFID and Beyond, S. 69.

[117] Vgl. hierzu auch Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 95.

der Kunde sich mittels seiner RFID getaggten Kundenkarte – über die das Alter des Kunden ermittelt werden kann – autorisiert.[118]

f) Bezahlvorgang

Für den Kunden könnte RFID insbesondere beim Bezahlen Vorteile bringen. Dies gilt nicht nur im Einzelhandel, sondern beispielsweise auch bei Mautsystemen. Sogar die „Geldbörse unter der Haut“[119] ist möglich.

Vorausgesetzt jedes Produkt im Supermarkt ist mit einem entsprechend leistungsstarken Tag ausgestattet, könnte ein Erfassen aller Produkte an der Kasse gleichzeitig erfolgen, indem der Kunde den Wagen lediglich durch eine Leseschranke schiebt. Das Einscannen der Strichcodes entfiele damit.

RFID Technik wird bereits in verschiedenen automatischen Maut-Systemen weltweit[120] verwendet. Ein Beispiel ist der E-ZPass[121], mit dem man in mehreren Bundesstaaten in den USA (New Jersey, New York, Massachusetts, Pennsylvania, Delaware, Maryland und West Virginia) automatisch seine Mautgebühren bezahlen kann. Auch mit dem französischen System Liber-T und dem italienischen SI Pass wird das Bezahlen an Maut-Stellen automatisiert. Die mit einem RFID-Tag ausgestatteten Fahrzeuge können durch ein spezielles Tor fahren, wobei ihr Tag gescannt wird und der fällige Mautbetrag mittels der im Hintergrundsystem gespeicherten Bankdaten von ihrem Konto abgebucht wird.[122] Eines der momentan größten automatischen RFID gestützten Bezahl-System ist der ExxonMobil Speedpass.[123] Mit diesem kann der Autofahrer automatisch an den teilnehmenden Tankstellen von Exxon und Mobil bezahlen.[124] Getestet wurden auch Kooperationen mit 450 McDonalds Filialen in Chicago und Northwest-Indiana, sowie 14 Stop&Shop Supermärkten im Raum Boston.[125] Dem Kunden wird ein RFID-Tag für den Schlüsselbund ausgehändigt, auf dem lediglich eine Identifikationsnummer sowie ein „Schlüssel“ gespeichert sind. Mittels Challenge-Response-Verfahren[126] wird die Authentizität des Tags überprüft und im Anschluss auf die im Hintergrundsystem

---

[118] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 7.

[119] Vgl. Der SPIEGEL, Ausgabe 23/2004 vom 29.05.2004, Börse unter der Haut, S. 156.

[120] Vgl. eine Auflistung bei *Langheinrich*, Gibt es in einer total informatisierten Welt noch eine Privatsphäre? *in*: Mattern (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, S. 240, abrufbar unter http://www.vs.inf.ethz.ch/res/papers/langhein-comp21-2007.pdf (04.04.2013).

[121] https://www.e-zpassny.com/en/home/index.shtml (04.04.2013).

[122] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 10.

[123] https://www.speedpass.com/ (04.04.2013), Der Pass findet Verwendung in den USA, Kanada, Singapur und Japan, vgl. Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007 oben Fn. 110, S. 9.

[124] Silicon.de News vom 09.02.2004, RFID ist für Verbraucher ein Buch mit sieben Siegeln, abrufbar unter http://www.silicon.de/enid/storage_network/6464 (04.04.2013).

[125] *Garfinkel*, RFID Payments at ExxonMobil *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 179.

[126] Hierzu mehr unten, E.II.4.b).

gespeicherten Kreditkarten- bzw. Bankkartendaten des Kunden zugegriffen.[127] Somit kann der Kunde nach dem Tanken einfach das Tag an den Reader an der Zapfsäule halten und die Transaktion wird durchgeführt.[128]

Sogar das Bezahlen mittels implantiertem RFID-Chip ist nicht mehr nur denkbar. Der Baja Beachclub mit Locations in Rotterdam und Barcelona bietet Stammgästen eine VIP-Mitgliedschaft an, die eine solche Implantierung beinhaltet.[129] Mit dem reiskorngroßen Chip, der den Gästen in den Oberarm eingepflanzt wird, können diese schnellen Zutritt zum Club erlangen, bekommen Einlass in den VIP-Bereich und können auch ihre Drinks auf diesem Weg bezahlen. Die Kellner halten zu diesem Zweck einen portablen Reader an den getaggten Oberarm des Kunden. Das passive Tag übermittelt hierbei seine Identifikationsnummer. Alle weiteren Informationen, wie Name und noch vorhandenes Guthaben, sind im IT-System des Clubs gespeichert.[130] Die VIP-Kunden des Baja Beachclubs sind von den RFID-Tags sehr angetan; das System vermittelt ein exklusives und sicheres Gefühl. *„The main benefit is that you can go out without having to carry a wallet, which can get easily lost in a night club. […]"*[131]

g) Reklamation und Rückgabe

Auch bei Reklamationen oder Rückgabe von Produkten kann RFID Vereinfachungen für den Kunden mit sich bringen. Bis dato muss ein Käufer theoretisch zwei Jahre lang den Kassenzettel zu einem Produkt aufheben, weil er in dieser Zeit von seinen gesetzlichen Gewährleistungsrechten Gebrauch machen kann. Hintergrund ist die Führung des Beweises, dass er das Produkt bei diesem Händler gekauft hat und die Gewährleistungsansprüche noch nicht verjährt sind. Diese Unannehmlichkeit könnte mittels RFID umgangen werden. Im Rahmen eines *Product Life Time Recording*[132] könnten die erforderlichen Daten einfach auf dem RFID-Tag des Produktes oder aber in der dazugehörigen Datenbank des Verkäufers gespeichert werden.[133] Ein Aufbewahren des Kassenzettels würde damit überflüssig. Allerdings muss dann natürlich das Tag im oder am Produkt aktiv und unversehrt bleiben.

---

[127] Interview mit Joe Giordano, Vize-Präsident der System- und Produkt-Entwicklung für Speedpass Network in der ExxonMobil Corporation, *Garfinkel*, RFID Payments at ExxonMobil *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 182.

[128] https://www.speedpass.com/forms/frmHowItWorks.aspx?pPg=howTech.htm&pgHeader=how (11.04.2012).

[129] SPIEGEL, Ausgabe 23/2004 vom 29.05.2004, Börse unter der Haut, S. 156.

[130] STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 19.

[131] Steve van Soest – einer der VIP-Gäste im Club in Rotterdam – im Rahmen der STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 19.

[132] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 61.

[133] *Albrecht/McIntyre*, Spychips, S. 79.

3. Authentisierung, Authentifizierung, Autorisierung

a) Elektronischer Türschlüssel

Viele Unternehmen haben im Rahmen der Zugangskontrolle von Schlüsseln oder Magnetkarten auf RFID Systeme umgestellt.[134] Die Angestellten erhalten eine RFID getaggte Karte oder ein Token ausgehändigt, mittels derer sie sich an entsprechenden Lesegeräten authentisieren und somit beispielsweise Türen öffnen können.

b) ÖPNV-Ticket

Der Einsatz von RFID im öffentlichen Personennahverkehr automatisiert das Bezahlen des Ticktes und die Überprüfung, ob der Fahrgast einen validen Fahrausweis besitzt, der ihn zum Besteigen des Transportmittels berechtigt.[135] Die getaggten Tickets können dabei entweder als Dauerkarten (Tages-, Wochen- oder Monatskarten) fungieren, bei denen gespeichert wird, für welchen Zeitraum und welches Gebiet im Vorfeld das Beförderungsentgelt bezahlt worden ist. Aber auch der Einsatz als Debit- oder Kreditkarte ist möglich. Debitkarten funktionieren wie Prepaid-Karten, d.h. die Karte muss vor der Nutzung am Schalter, am Automaten oder vom heimischen PC aus aufgeladen werden. Im Verlauf wird dann pro Fahrt der entsprechende Betrag abgebucht, indem der Fahrgast beim Betreten und Verlassen des Beförderungsmittels sein Ticket an ein entsprechendes Lesegerät hält. Gleichermaßen kann auch mittels Kreditkarte der jeweilige Betrag eingezogen werden. In diesem Fall ist allerdings kein Guthaben auf der Karte selbst gespeichert, sondern über gespeicherte Bankdaten im Hintergrund kann eine automatische Abbuchung vom Konto des Kunden erfolgen.[136]

Der Verkehrsbund Rhein Ruhr in Nordrhein-Westfalen führte 2003 RFID getaggte Fahrkarten im öffentlichen Personennahverkehr ein.[137] Laut der Website des VRR[138] werden auf den Karten nicht nur Daten zur Gültigkeitsdauer des Fahrausweises sondern auch Name und Geburtsdatum des Besitzers gespeichert. Die RFID-Tags entsprächen den Vorgaben der ISO 14443[139], die bestimmte maximale Sendereichweiten für RFID Systeme festlegt. Dementspre-

---

[134] STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 20.

[135] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zum „Einsatzgebiet eTicketing im öffentlichen Personennahverkehr“ 2008 eine „TR RFID – Technische Richtlinie für den sicheren RFID-Einsatz“ herausgegeben, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03126/BSI-TR-03126-1_pdf.pdf;jsessionid=574B87E22A2867D6824C01896F12C9FF.2_cid156?__blob=publicationFile (04.04.2013).

[136] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 11.

[137] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 11.

[138] Vgl. die Broschüre zum Ticket1000, abrufbar unter http://www.vrr.de/blaetterkatalog/Ticket1000_2012/blaetterkatalog/ (04.04.2013), S. 10.

[139] “ISO/IEC 14443-1:2008 defines the physical characteristics of PICCs, commonly known as proximity cards. It is to be used in conjunction with other parts of ISO/IEC 14443”, vgl. offizielle Homepage der International Standardization Organization http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39693 (04.04.2013).

chend läge die maximale Lesereichweite bei ca. 10 Zentimetern. Ein Auslesen durch Dritte sei damit in der Praxis kaum zu erwarten. Auch der VRR selbst würde mit den neuen Fahrkarten keine Bewegungsmuster seiner Kunden anfertigen. Dies sei ohnehin vertraglich festgelegt.

Im Jahr 2004 führte das Londoner Verkehrsunternehmen Transport for London (TfL)[140] die RFID getaggte *Oyster Card*[141] ein. Auch auf dieser Karte sind bestimmte Kundendaten gespeichert.

In den Niederlanden ist sogar ein einheitliches landesweites eTicketing-System geplant[142] – die *OV-Chipkaart*.[143] Auch hier werden RFID getaggte Fahrkarten an die Kunden ausgegeben. Es besteht grundsätzlich die Wahlmöglichkeit zwischen anonymen und personalisierten Fahrkarten. Auf letzteren werden persönliche Daten wie Name, Geburtsdatum etc. gespeichert.[144]

c) WM-Tickets

Zur Fußball-Weltmeisterschaft 2006 gab das FIFA Worldcup Ticketing Center erstmals RFID getaggte Tickets an die Besucher aus. Damit sollte sichergestellt werden, dass nur der berechtigte Karteninhaber auch ins Stadion konnte und eine möglichst große Fälschungssicherheit erreicht werden. Auch ein Abgleich mit der Hooligan-Datei im Vorfeld der Spiele sollte so ermöglicht werden. Auf dem Tag in der Karte war nur eine Identifikationsnummer gespeichert.[145] Die beim Kauf angegebenen Daten – Name, Adresse, Geschlecht, Geburtstag, Passnummer und evtl. auch E-Mail-Adresse und Telefonnummer – wurden hingegen nur in einer Datenbank im Hintergrundsystem gespeichert. Beim Einlass am Stadion wurde dann das RFID-Tag gelesen und mit den gespeicherten Daten abgeglichen. Ein weiteres Lesen des Tags fand hingegen nicht statt.[146]

d) Ski-Pass

Ein RFID-Tag auf dem Skipass ermöglicht mittlerweile in vielen Skigebieten die Benutzung der Liftanlagen ohne mühseliges Suchen des Tickets.[147] Ein Vorbeiführen des in der Jacken-

---

[140] http://www.tfl.gov.uk/home.aspx (04.04.2013).

[141] Vgl. BBC News vom 25.09.2003, Smart Cards Track Commuters, abrufbar unter http://news.bbc.co.uk/2/hi/technology/3121652.stm (04.04.2013).

[142] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 13.

[143] http://www.ov-chipkaart.nl/ (04.04.2013).

[144] Vgl. für weitere Beispiele im ÖPNV-E-Ticketing *Langheinrich*, Gibt es in einer total informatisierten Welt noch eine Privatsphäre? *in*: Mattern (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, S. 241, oben Fn. 120.

[145] *Holznagel/Bonnekoh*, MMR 2006, 17 (21).

[146] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 18; *Weichert*, ULD Schleswig-Holstein, Die Fußball-WM als Überwachungs-Großprojekt, abrufbar unter https://www.datenschutzzentrum.de/allgemein/wmticket.htm (04.04.2013)

[147] Vgl. hierzu auch *Langheinrich*, Gibt es in einer total informatisierten Welt noch eine Privatsphäre? *in*: Mattern (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, S. 240, oben Fn. 120.

tasche befindlichen Passes an einem Lesegerät erspart das Ausziehen der Handschuhe und Hantieren mit dem Reißverschluss. Mittels des Snowpass Access Systems von Swatch[148] kann der Besitzer einer entsprechenden Armbanduhr seinen Skipass sogar auf das in dieser Uhr integrierte Tag speichern lassen. Ähnliche Systeme werden auch von verschiedenen Anbietern in Handschuhe integriert.

e) Elektronische Wegfahrsperre

In der Automobilindustrie wird RFID schon seit 1995 in Form der automatischen Wegfahrsperre als Authentifizierungsmerkmal verwendet.[149] In den Autoschlüssel wird ein RFID-Tag eingebaut, das vor dem Anlassen des Motors von einem Reader dahingehend überprüft wird, ob es sich bei dem verwendeten auch um den „berechtigten" Schlüssel handelt. Nur bei erfolgreicher Authentifizierung wird das Starten des Motors zugelassen. Nicht zu verwechseln ist dieser Vorgang mit der Fernsteuerung zur Öffnung der Türschlösser. Diese ist zwar ebenfalls in den Autoschlüssel integriert, funktioniert aber nicht mittels RFID. Durch Druck auf den Transmitter werden verschlüsselte Funk- oder Infrarotimpulse an den Empfänger im Auto gesendet.[150]

4. Medizinische Notfälle

Die für die Implantierung im Baja Beachclub verwendeten VeriChips sind ursprünglich für das Gesundheitswesen entwickelt worden. Eingesetzt werden sollen sie nach Informationen der offiziellen Website[151] des Unternehmens zur Patientenidentifikation. Denkbar ist aber auch eine automatische „Anwesenheitskontrolle" z.B. in Altersheimen. Die auf dem VeriChip gespeicherte Nummer dient als Schlüssel zu den Informationen, die in einer externen Datenbank gespeichert sind.[152] Insbesondere in Notfallsituationen, in denen sich der Patient nicht mehr selbst mitteilen kann – wie Schlaganfall, diabetesbedingter Schock, schwerer Herzinfarkt, epileptischer Anfall – kann der behandelnde Notarzt durch das Auslesen der VeriChip-Nummer und Einsichtnahme in die hierzu gespeicherten Daten wichtige und vielleicht lebensrettende Informationen für die Behandlung des Patienten gewinnen. Gerade bei Risikopatienten oder Patienten mit angeborenen schweren Krankheiten bietet sich die Implantierung des VeriChip damit an. Sie ist in jedem Lebensstadium also auch unmittelbar nach der Geburt denkbar. Der Betreffende trüge dann den VeriChip potenzieller Weise sein ganzes Leben

---

[148] http://www.swatch.com/zz_en/snowpass.html (11.04.2012).

[149] Verband der Automobilindustrie, Jahresbericht 1999, abrufbar unter http://www.vda.de/de/publikationen/jahresberichte/ (04.04.2013), S. 178

[150] *Langheinrich*, Gibt es in einer total informatisierten Welt noch eine Privatsphäre? *in*: Mattern (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, S. 239, oben Fn. 120.

[151] Das Unternehmen *VeriChip* heißt mittlerweile *PositiveID*, Webseite abrufbar unter http://www.positiveidcorp.com/index.html (04.04.2013).

[152] *Heinrich* (Hrsg.), RFID and Beyond, S. 179.

lang. Die U.S. amerikanische Food and Drug Administration (FDA) hat im Oktober 2004 die Implantierung des VeriChips in Menschen befürwortet.[153]

5. Ausweisdokumente

a) Europa

Seit dem 28. August 2006 sind alle Mitgliedstaten der Europäischen Union verpflichtet die Regelungen der Verordnung (EG) Nr. 2252/2004[154] anzuwenden. Die Verordnung verpflichtet die Mitgliedstaaten zur Einführung des biometrischen Reisepasses.[155]

> Art. 1 Abs. 2 S. 1 (EG) Nr. 2252/2004
>
> Die Pässe und Reisedokumente sind mit einem Speichermedium versehen, das ein Gesichtsbild enthält. Die Mitgliedstaaten fügen auch Fingerabdrücke in interoperablen Formaten hinzu.

Die Verordnung ist eine Reaktion auf die Spezifikationen der International Civil Aviation Organisation (ICAO) zu maschinenlesbaren Reisedokumenten[156], nämlich die Ausstattung der Reisedokumente mit Gesichtserkennungsmerkmalen.[157] Das von der Verordnung geforderte Speichermedium ist ein RFID-Tag.[158] Auf ihm gespeichert werden ein Foto in Frontalaufnahme sowie zwei Fingerabdrücke. Weitere biometrische Merkmale wie DNA-Profil oder Iris-Scan können ergänzt werden. In Deutschland wurde das Foto seit dem ersten Tag der Ausgabe des neuen Passes auf dem Chip gespeichert. Die Speicherung der Fingerabdrücke trat erst im November 2007 hinzu.[159]

---

[153] U.S. Food and Drug Administration, Doc. No. 2004N–0477, Medical Devices; General Hospital and Personal Use Devices; Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information, Federal Register, Vol. 69, No. 237, vom 10.12.2004, abrufbar unter http://www.fda.gov/ohrms/dockets/98fr/04-27077.pdf (04.04.2013), S. 71702; U.S. Food and Drug Administration, Doc. 1541 vom 10.12.2004, Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information, abrufbar unter http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm072141.htm (04.04.2013).

[154] Verordnung (EG) 2252/2004 des Rates vom 13. 12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. L 385 vom 29.12.2004 S. 1 ff., abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:de:HTML (04.04.2013).

[155] Die Frage der Gültigkeit von Art. 1 Abs. 2 der Verordnung (EG) Nr. 2252/2004 hat das VG Gelsenkirchen dem EuGH vorgelegt, Beschl. v. 15.05.2012 – 17 K 3382/07, NVwZ 2012, 982. Der Kläger hat bei der Beklagten die Erteilung eines Reisepasses beantragt, wobei er die Erfassung seiner Fingerabdrücke verweigerte.

[156] International Civil Aviation Organization (ICAO), Doc. 9303, Machine Readable Travel Documents, 6th edition 2006, abrufbar unter http://www.icao.int/publications/Documents/9303_p1_v1_cons_en.pdf (04.04.2013).

[157] Vgl. Erwägungsgrund 3 der Verordnung (EG) 2252/2004 des Rates vom 13. 12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. L 385 vom 29.12.2004 S. 1 ff., oben Fn. 154.

[158] Vgl. Informationen zum elektronischen Reisepass auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik, abrufbar unter https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/ePass/epass_node.html (04.04.2013).

[159] Vgl. Informationen zum elektronischen Reisepass auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik, oben Fn. 158.

Der deutsche Gesetzgeber hat einen von der Bundesregierung eingeführten Gesetzentwurf[160] zur Änderung des Passgesetzes und anderer Gesetze verabschiedet. Der E-Pass ist seit dem Inkrafttreten der Änderung am 01.11.2007 auch im deutschen Recht enthalten.

> § 4 Abs. 3 S. 1 PassG
>
> Auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABl. EU Nr. L 385 S. 1) sind der Reisepass, der Dienstpass und der Diplomatenpass mit einem elektronischen Speichermedium zu versehen, auf dem das Lichtbild, Fingerabdrücke, die Bezeichnung der erfassten Finger, die Angaben zur Qualität der Abdrücke und die in Absatz 2 Satz 2 genannten Angaben gespeichert werden.

Mit dem Änderungsgesetzt wurde gleichzeitig auch das Personalausweisgesetz geändert. Seit dem 01.11.2010 werden auch Personalausweise mit einem RFID-Chip ausgegeben, auf dem wiederum Lichtbild und auf Antrag der antragstellenden Person auch die Fingerabdrücke gespeichert werden.[161] Neben dem Lichtbild und den Fingerabdrücken werden auf dem E-Pass und dem E-Perso aber auch die bisher üblichen Passdaten – also Name, Geburtstag und -ort, Adresse etc. – gespeichert, vgl. § 4 Abs. 3 S. 1 PassG, § 5 Abs. 5 Nr. 1 PAuswG.[162]

b) USA

Auch in den USA werden bereits seit 2005 biometrische Daten mittels RFID-Tag in Pässe eingebracht.[163] Tatsächlich stützt sich die gesamte Biometrie-Debatte auf Forderungen der USA nach 9/11 in alle Reisedokumente biometrische Daten aufzunehmen.[164]

Auch in die als „faktische ID-Karten“[165] bezeichneten neuen amerikanischen Führerscheine müssen „*machine-readable technolog(ies)*“ integriert werden.[166] Dies wurde durch den Real-ID-Act von 2005[167] geregelt. Was genau diese Technologien alles sein können, legt der Gesetzgeber nicht fest. Dem Wortlaut der Norm nach kommt RFID Technik aber zumindest in

---

[160] Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften, BRDrucks 16/07 vom 05.01.2007, abrufbar unter http://dipbt.bundestag.de/dip21/brd/2007/0016-07.pdf (04.04.2013).

[161] Heise News Meldung vom 09.10.2007, SPD gibt Widerstand gegen Fingerabdrücke in Personalausweisen auf, http://www.heise.de/newsticker/meldung/97138 (04.04.2013).

[162] Vgl. auch die Informationen zum elektronischen Reisepass auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik, oben Fn. 158.

[163] Vgl. *Heinrich* (Hrsg.), RFID and Beyond, S. 178.

[164] In ihrem nach 9/11 verabschiedeten „Enhanced Border Security and Visa Entry Reform Act“ forderten die USA von den 25 Partnern des Visa-Waiver-Abkommens biometrische Daten in ihre Pässe einzuführen, wenn ihre Staatsangehörigen weiterhin ohne Visa in die USA einreisen können sollten, vgl. *Roßnagel*, DuD 2005, 69 (60).

[165] EPIC, National ID Cards and Real ID Act, http://www.epic.org/privacy/id_cards/ (04.04.2013).

[166] “RealID Act of 2005” (H.R. 418, 2005), später Title II of the “Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005” (H.R. 1268, 2005, SEC. 202. MINIMUM DOCUMENT REQUIREMENTS AND ISSUANCE STANDARDS FOR FEDERAL RECOGNITION, (b) (9): “Minimum Document Requirements- To meet the requirements of this section, a State shall include, at a minimum, the following information and features on each driver's license and identification card issued to a person by the State: […] A common machine-readable technology, with defined minimum data elements.”.

[167] “RealID Act of 2005” (H.R. 418, 2005), später Title II of the “Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005” (H.R. 1268, 2005).

Betracht. Auch das für die Spezifizierungen zum Real-ID-Act zuständige Department of Homeland Security (DHS) nennt RFID als eine mögliche Technik, um den gesetzlichen Forderungen nach Maschinenlesbarkeit von Identifikationsdokumenten gerecht zu werden.[168] Allerdings befindet es RFID als unangemessen für die flächendeckende Verwendung in Führerscheinen. Es sei nicht erkennbar, warum Reisedokumente dauerhaft und regelmäßig kontaktlos über eine gewisse Entfernung ausgelesen werden müssten.[169] Dennoch hat der Staat Washington als Pionier bereits den RFID Führerschein eingeführt.[170]

Auf Staatenebene regt sich herber Widerstand gegen die *Enhanced Driver's License*. Mehrere Staaten haben bereits Gesetzte verabschiedet, die ausdrücklich die Umsetzung des Real-ID-Acts in dieser Hinsicht verhindern. Andere folgen dem Vorbild und arbeiten an entsprechenden Regelungen.[171] Es gibt unterschiedliche Beweggründe für ein solches Verhalten der Staaten. Auf der einen Seite steht die Finanzierung des von der U.S. Regierung unter Bush geforderten Neuerungen durch Real-ID. Anderseits ist aber auch die drohende Registrierung aller U.S. Bürger in einem einheitlichen System – das zumindest einen Datenaustausch unter den Staaten ermöglichen soll – einer der Reizpunkte, die Real-ID an der Umsetzung hindert.

6. Haushaltsgegenstände

Smarte Haushaltsgegenstände sind eine weitere Anwendungsmöglichkeit. Die RFID-Tags auf den im Supermarkt oder Kaufhaus gekauften Gegenständen können theoretisch auch im eigenen Zuhause noch Verwendung finden. Man stelle sich zum Beispiel den intelligenten – sprich mit einem Lesegerät ausgestatteten – Kühlschrank[172] vor, der automatisch erkennt, dass die Milch abgelaufen ist und sofort neue beim Supermarkt bestellt. Oder aber die smarte Waschmaschine, die anhand der Tags in den Kleidungsstücken weiß, welches Waschprogramm sie zu wählen hat.

In der Abfallentsorgung werden bereits RFID getaggte Mülltonnen eingesetzt.[173] Die Vorteile sind eine verbesserte Behälterlogistik, die Vermeidung von Leistungsmissbrauch (nicht an-

---

[168] U.S. Department for Homeland Security (DHS), Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, "Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes", abrufbar unter http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (04.04.2013), S. 75.

[169] U.S. Department for Homeland Security (DHS), Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, "Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes", oben Fn. 168, 76.

[170] Seattle Post Intelligencer Online, Meldung vom 23.03.2007, New driver's license OK'd for border, abrufbar unter http://seattlepi.nwsource.com/local/308864_border24.html (04.04.2013).

[171] Für eine Übersicht über Anti-RealID-Gesetzgebung, Stand 2009 vgl. eine Website der American Civil Liberties Union (ACLU), http://www.realnightmare.org/news/105/ (04.04.2013).

[172] Vgl. zum „Intelligent Fridge" *Rothensee*, User Acceptance of the Intelligent Fridge: Empirical Results from a Simulation *in*: Flörkemeier/Langheinrich/Fleisch/Mattern/Sarma, The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 123 ff.

[173] In einigen bayrischen Landkreisen ist dies der Fall; vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 70. An der ETH Zürich wurde ein solches „Intelligent Waste Management System" (BIN IT!) entwickelt, vgl. http://www.embedded-wisents.org/competition/pdf/schoch.pdf (04.04.2013).

gemeldete und damit auch nicht der Abrechnung unterfallende Mülltonnen würden vom smarten Müllwagen erkannt) sowie individuellere und damit genauere Abrechnungen und Gebührenbescheide (der Bürger bekommt nur so viele Leerungen in Rechnung gestellt, wie auch tatsächlich stattgefunden haben).

7. Implantierung in Tiere

Die genaue Identifizierung von Nutztieren[174], insbesondere Schlachtvieh, ist bei steigender Anzahl von Tierseuchen – BSE, Vogelgrippe, Schweinepest – von immenser Bedeutung. Verbraucher machen ihre Forderung nach mehr Transparenz deutlich, indem sie auf Bio-Produkte umsteigen und der Massentierhaltung zunehmend den Rücken kehren. Auch seitens der Politik werden immer höhere Anforderungen an die Nachvollziehbarkeit des Werdegangs der Tiere gestellt. Der europäische Gesetzgeber hat erkannt, welche Vorteile eine RFID gestützte Tieridentifikation bringt. Der Europäische Rat hat entsprechend[175] im Dezember 2003 eine Verordnung[176] erlassen, in der die gesetzliche Pflicht für bestimmte Züchter normiert wird, ihre Zuchttiere[177] mit „Transpondern" zur Identifikation zu versehen.

> Art. 4 der Verordnung (EG) 21/2004
>
> (2) a) Die Tiere werden gekennzeichnet durch ein erstes Kennzeichen, das die im Anhang unter Abschnitt A Nummern 1 bis 3 genannten Anforderungen erfüllt.
>
> b) Die Tiere werden gekennzeichnet durch ein zweites Kennzeichen, das von der zuständigen Behörde genehmigt wurde und die im Anhang unter Abschnitt A Nummer 4 aufgeführten technischen Anforderungen erfüllt. (…)
>
> Anhang
>
> A. Kennzeichen
>
> (…)
>
> 4. Als zweites Kennzeichen gemäß Artikel 4 Absatz 2 Buchstabe b) kann Folgendes gewählt werden:
>
> (…)
>
> - ein **elektronischer Transponder** [Hervorh. eingef. d. Verf.] mit den unter Nummer 6 aufgeführten Eigenschaften.
>
> (…)
>
> 6. Die elektronischen Kennzeichen erfüllen die folgenden technischen Normen:
>
> - Es handelt sich um Nurlese-Passivtransponder mit der den ISO-Normen 11784 und 11785 entsprechender HDX- oder FDX-B-Übertragung.
>
> - Sie sind mit der ISO-Norm 11785 entsprechenden Lesegeräten ablesbar, d. h. HDX- oder FDX-B-Übertragung zwischen Lesegerät und Transponder ist gewährleistet.

---

[174] Vgl. auch *Holznagel/Bonnekoh*, MMR 2006, 17 (19).

[175] Der Gesetzgebung voran ging ein Projekt der Europäischen Kommission namens IDEA (Electronic Identification of Animals), im Rahmen dessen die Kennzeichnung von Tieren mittels RFID-Technik erprobt wurde, vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 76 ff.

[176] Verordnung (EG) Nr. 21/2004 des Rates vom 17. Dezember 2003 zur Einführung eines Systems zur Kennzeichnung und Registrierung von Schafen und Ziegen und zur Änderung der Verordnung (EG) Nr. 1782/2003 sowie der Richtlinien 92/102/EWG und 64/432/EWG, ABl. L 005 vom 09.01.2004, S. 8 – 17, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0021:DE:HTML (04.04.2013).

[177] Die Verordnung (EG) 21/2004, oben Fn. 176, beschränkt sich auf Ziegen und Schafe.

> - Die Lesereichweite beträgt im Falle von Handlesegeräten bei Ohrmarken mindestens 12 cm und bei Bolustranspondern mindestens 20 cm, im Falle stationärer Lesegeräte bei Ohrmarken und Bolustranspondern mindestens 50 cm.

Allen Seiten ist daran gelegen, auf lückenlose „Lebensläufe" der Tiere zurückgreifen zu können. Mittels RFID gestützter Systeme lässt sich dies einfach bewerkstelligen. Jedes Tier erhält nach der Geburt ein Tag implantiert oder auf anderem Wege dauerhaft mit dem Körper verbunden. Auf dem Tag können entweder direkt Daten zur Herkunft, bisherigen Krankheiten, Alter etc. gespeichert werden, oder aber es kann wiederum lediglich eine Identifikationsnummer enthalten sein, zu der dann die weiteren Informationen im Hintergrundsystem gespeichert werden. Auf einem internationalen Markt erscheint die zweite Lösung praktikabler, weil dann keine gemeinsame Datenbank erforderlich ist, sondern die Daten immer direkt einsehbar sind.

Auch die Implantierung von RFID Chips in Haustiere findet heute regelmäßig statt. In diversen Hundegesetzen finden sich mittlerweile entsprechende Regelungen. So z.B. in Hamburg[178], in Nordrhein-Westfalen[179] oder auch in Berlin[180]. Das Berliner Hundegesetz beinhaltet folgende Regelung, die auch das grundsätzliche Verbot statuiert, die Identifikationsnummer auf dem RFID-Tag mit personenbezogenen Daten des Halters zusammen zu speichern:

> § 1 BlnHundeG Halten und Führen von Hunden
>
> (5) Hunde sind mit einem Chip gemäß ISO-Norm fälschungssicher zu kennzeichnen. Der zuständigen Behörde ist auf deren Verlangen die Chipnummer mitzuteilen oder der Hund zum Auslesen des Chips vorzuführen. Dabei sind die Hundehalter und Hunde führenden Personen verpflichtet, das Auslesen der Chipnummer zu dulden und zu unterstützen. Die zuständige Behörde speichert die Chipnummer, insbesondere in Verbindung mit personenbezogenen Daten des Hundehalters und weiteren Daten des Hundes, nur im Einzelfall. Für die Erhebung, Speicherung, Nutzung und Übermittlung dieser Daten durch die zuständige Behörde gelten die Regelungen des § 11.

III. Ubiquitärer Einsatz von RFID

Zwar sind die Prognosen, die an die Verbreitung von RFID insbesondere auf Produktebene gestellt wurden, nicht voll erfüllt worden – die Technik hat bis heute nicht, wie vielerorts erwartet, den Barcode vollständig abgelöst. Dies liegt zum einen sicherlich an den immer noch (zu) hohen Kosten für einen flächendeckenden Rollout. Auch die nur schleppend vorangehende Standardisierung und die sich aus der Beteiligung einer Vielzahl betroffener Staaten und ihrer Frequenzpolitik ergebenden Hemmnisse spielen eine Rolle. Einer der wesentlichsten Faktoren dürfte aber die Frage der Endkundenakzeptanz sein – und diese steht und fällt mit dem Umgang mit datenschutzrechtlichen Herausforderungen.[181]

---

[178] § 11 i.V.m. § 6 HambHundeG, HmbGVBl. 2006, S. 37, abrufbar unter http://www.landesrecht.hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-HuGHArahmen&doc.part=X&doc.origin=bs&st=lr (04.04.2013).

[179] § 4 Abs. 1 Nr. 6, Abs. 7 LHundG NRW, GVBl. 2002, S. 656, abrufbar unter http://www.umwelt.nrw.de/verbraucherschutz/pdf/lhg1_06.pdf (04.04.2013).

[180] § 1 Abs. 5 BlnHundeG, GVBl. 2004 S. 424, abrufbar unter http://www.berlin.de/imperia/md/content/sen-verbraucherschutz/lesefassunghundegesetz.pdf?start&ts=1178539344&file=lesefassunghundegesetz.pdf (04.04.2013).

[181] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 100.

Die Zeichen stehen dennoch dafür, dass ein Umstieg auf RFID in der Zukunft erfolgen wird.[182] Im Bekleidungssektor ist GERRY WEBER mit seiner RFID-Initiative diesen Schritt bereits gegangen. Das Unternehmen taggt mittlerweile all seine Produkte mit RFID und verwendet RFID-Technik in allen eigenen HOUSES of GERRY WEBER. *Dr. David Frink* aus dem Vorstand von Gerry Weber führt auf der Website des Unternehmens aus:

> „Mittlerweile ist unsere gesamte Kollektion mit RFID-Tags ausgestattet. Wir sind überzeugt, dass es in den nächsten Jahren einen hohen Durchdringungsgrad mit RFID in der Bekleidungsbranche geben wird. Als Vorreiter der Branche leben wir das jetzt schon. Gerry Weber ist der erste Mode-Hersteller, der die textile Kette durchgängig von der Produktion bis zum POS mit RFID unterstützt und dabei eingenähte Tags einsetzt.“[183]

Neben Gerry Weber hat auch C&A angekündigt, künftig seine Produkte flächendeckend mit RFID ausrüsten zu wollen. Im Sommer 2012 hat das Unternehmen in fünf Filialen begonnen den Einsatz von RFID zu testen.[184] Die Kleidungsstücke werden hierfür mit einem eingenähten RFID-Tag, ähnlich der Waschanleitung, ausgestattet.[185] Inzwischen findet die Technik auch in anderen Filialen Anwendung.[186]

Zwar bestehen zwischen Bekleidung und anderen Einzelhandelsprodukten insbesondere den Wert betreffend deutliche Unterschiede. Bei fallenden Stückpreisen ist davon auszugehen, dass eine großflächige Bestückung auch von niedrigpreisigen Produkten mit passiven Tags stattfinden wird.

Dies unterstreichen die Entwicklungen bei METRO. In den METRO Märkten der METRO GROUP findet RFID zunehmen Einsatz. Auf der Website des METRO Futur Stores erklärt das Unternehmen:

> „Die Einführung der Technologie geht mit großen Schritten voran.“[187]

Eine Stagnation kann entsprechend mitnichten festgestellt werden. Die Entwicklung hat sich eventuell verlangsamt. Und die Weiterverbreitung und die Entwicklungen im Bereich RFID bekommen lange nicht mehr die Aufmerksamkeit geschenkt, wie noch vor einigen Jahren. Diesseits wird aber davon ausgegangen, dass es ein „Zurück“ nicht geben wird. Die datenschutzrechtlichen Herausforderungen werden mit zunehmender Verbreitung dringlicher.

---

[182] Ähnlich auch *Huber*, MMR 2008, VI.

[183] Vgl. die offizielle Website von Gerry Weber, abrufbar unter http://www.gerryweber.com/ag-website/de/startseite/unternehmen/unternehmensprofil/innovationen/rfid (04.04.2013).

[184] C&A Pressemitteilung vom 01.06.2012, abrufbar unter http://www.c-and-a.com/de/de/corporate/fileadmin/mediathek/de-de/Pressemitteilungen/C-und-A_startet_RFID-Projekt_an_f%C3%BCnf_Standorten.pdf (04.04.2013).

[185] Dies hat jedenfalls eine Überprüfung in der Berliner Filiale am KuDamm-Eck Anfang Februar 2013 ergeben. Laut der Pressemitteilung von C&A werden die RFID-Tags (möglicherweise künftig?) außen mit Plastik-Strings an der Ware befestigt.

[186] Eine Liste findet sich auf der Website von C&A, abrufbar unter http://www.c-and-a.com/de/de/corporate/fashion/wir-fuer-sie/informationen-zu-rfid/ (04.04.2013). Hier finden sich auch Kundeninformationen über RFID, so u.a. der Hinweis, dass die Tags unmittelbar nach dem Einkauf entfernt werden können.

[187] Homepage des Metro Future Store, abrufbar unter http://future-store.org/fsi-internet/html/de/1564/index.html (04.04.2013)

C. Szenarien

Im folgenden Teil werden zunächst vier Szenarien kategorisiert, unter die die oben dargestellten Anwendungsbereiche subsumiert werden können. Im Anschluss werden vier *Leading Scenarios* herausgearbeitet, die im weiteren Teil der Arbeit Ausgangspunkt für die rechtliche Bewertung sein werden.

I. Kategorien

Die oben dargestellten Anwendungsbereiche lassen sich unter die folgenden Szenarien subsumieren: EPC (*Electronic Product Code*), RTAMP (*Real Time Authentication and Monitoring of Persons*), RTAMA (*Real Time Authentication and Monitoring of Animals*) sowie AGG (Aggregationsszenarien).[188] Teilweise kann es zu Überschneidungen bei der Einordnung kommen.

1. EPC

EPC steht für *Electronic Product Code*. Es handelt sich hierbei um ein AutoID- (*automatic identification*) System. Entwickelt wurde das Konzept vom *AutoID-Center*[189] des Massachusetts Institute of Technology (MIT), Cambridge (USA). Verwaltet wird es jetzt von EPCglobal Inc.[190], einem Zusammenschluss des Uniform Code Council (UCC)[191] und *EAN* International.[192] In Deutschland wird EPCglobal durch das Industriestandardisierungsgremium *GS1 Germany* vertreten.[193] Unterstützt wird die Organisation von über 100 „End-User-Sponsoren" aus dem wirtschaftlichen[194] aber auch dem öffentlichen[195] Bereich.

---

[188] Diese Einteilung hat bereits vorgenommen *Schmid*, Mastering the Legal Challenges *in*: Heinrich (Hrsg.), RFID and Beyond, S.193 ff.

[189] Vgl. die offizielle Website des MIT, abrufbar unter http://autoid.mit.edu/cs/ (04.04.2013).

[190] Vgl. die offizielle Website von EPCglobal, abrufbar unter http://www.epcglobalinc.org/home (04.04.2013).

[191] Von UCC stammt bereits auch schon der „Vorgänger" des EPC, der UPC (Universal Product Code), der Grundlage für die Warenerkennung mittels Barcode ist.

[192] *Sarma*, A History oft he EPC *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 53; *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 88.

[193] Vgl. die offizielle Homepage von GS1, abrufbar unter http://www.gs1-germany.de/gs1-standards/barcodesrfid/epcrfid/ (04.04.2013).

[194] U.a. seien hier genannt Coca-Cola, Gillette, Procter & Gamble, Wal-Mart, vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 30; *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 88.

[195] So z.B. die U.S. Food and Drug Administration (FDA) sowie das U.S. Verteidigungsministerium (Department of Defense), vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 29; *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 88.

Die Besonderheit des EPC ist die Zuteilung einer einzigartigen, nach einem speziellen Schema aufgebauten Identifikationsnummer zu einem Produkt. Gleichzeitig hält das EPC Rahmenprogramm aber auch Standards für Tags, Reader sowie Hintergrundsysteme bereit.[196]

Der Unterschied zum weltweit verwendeten Barcode[197] liegt darin, dass Produkte nicht mehr nur einer bestimmten Produktgruppe zugeordnet werden können, sondern dass jedes einzelne Produkt eine eigene Identifikationsnummer erhält.[198] Motivation für alle AutoID-Systeme[199] ist die Vereinfachung der Produktidentifikation. Diese nimmt in der Herstellungs- und Lieferkette einen großen Stellenwert ein, um logistische Abläufe möglichst fehlerfrei und effizient gestalten zu können. Der Barcode hat in dieser Hinsicht bereits revolutionäre Vereinfachungen mit sich gebracht. Bestehend aus einem binären Strich-Code, der durch ein Lesegerät visuell abgetastet wird, übermittelt der Barcode eine Produktinformationsnummer an das mit dem Lesegerät verbundene IT-System. Der Barcode beschränkt sich dabei auf die Speicherung einer Herstellerkennung sowie einer Produktnummer. Bekannt dürfte jedem der Barcode aus dem Einzelhandel sein, dem letzten Schritt in der Lieferkette. Ohne Barcode würde insbesondere der Bezahlvorgang wesentlich viel länger dauern. Der Barcode ordnet ein Produkt einem bestimmten Unternehmen sowie einer bestimmten Produktgruppe zu und lässt die Verknüpfung mit einem bestimmten Verkaufspreis zu, der beim Scannen an der Kasse aufleuchtet. Die verwendete Nummer basiert auf einem System namens Universal Product Code (UPC)[200]. Gleiche Produkte haben alle denselben Code. Der Barcode und die von ihm vermittelten Informationen sind ausreichend in Systemen, in denen es nicht auf die genaue Identifizierung des einzelnen Produkts ankommt, sondern vielmehr die Zuordnung des Artikels zu einer bestimmten Produktgruppe genügt.

Das AutoID-Center hat eine weiter reichende Vision: Jedes Produkt soll bereits bei seiner Herstellung mit einem RFID-Tag ausgestattet werden, auf dem eine EPC-Nummer gespeichert ist. EPC als globaler Standard vorausgesetzt wäre damit eine eindeutige Identifikation jedes Produkts weltweit möglich – dies ist eine der Grundvoraussetzungen der Idee eines *Internet of Things*. Das AutoID-Team ging bei der Entwicklung von EPC von der Überlegung aus, dass es sinnvoll ist, nur wenige Daten auf dem Tag selbst zu speichern und statt Größe und Kosten in die Höhe zu treiben eine Verknüpfung mit externen Datenbanken herzustel-

---

[196] *Heinrich* (Hrsg.), RFID and Beyond, S. 104.

[197] Das erste Barcode-Patent wurde 1949 angemeldet; die heute bekannten linearen Barcodes wurden erst in den späten 1960er Jahren verstärkt eingesetzt, vgl. *Mullen/Moore*, Automatic Identification and Data Collection: What the Future Holds *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 4. Speziell für den Lebensmittelhandel entwickelt wurde der EAN-(European Article Number)Code, vgl. *Finkenzeller*, RFID-Handbuch, S. 3; auch UPC – Universal Product Code, *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 27.

[198] *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 88.

[199] Weitere AutoID-Systeme sind z.B. Chip Card gestützte Systeme, *Heinrich* (Hrsg.), RFID and Beyond, S. 87 f.; aber auch mechanische, elektromechanische oder magnetische Identifikationssysteme, *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 136 f.

[200] Vgl. schon Fn. 191.

len.[201] Diese Datenbank soll aus einem ganzen Netzwerk von Computern bestehen – dem Object Name Service (ONS).[202] Es besteht aus zentralen „*root*"-Servern und lokalen Servern bei den verschiedenen Herstellern. Wird ein Produkt an der Kasse eines Einzelhändlers gescannt, schickt das Kassensystem eine Anfrage an den *root*-Server. Dieser hat bereits erste Informationen über das Produkt gespeichert, nämlich von welchem Hersteller es kommt.[203] Mit dieser Information wendet sich das Kassensystem dann an den Server des entsprechenden Herstellers und fragt dort erneut an.[204] Auf dem Server des Herstellers sind alle Informationen gespeichert und können jeweils passend auf die Anfrage erteilt werden. Geplant ist, dass jedes Produkt seine eigene Website bekommt, auf der die relevanten Informationen eingesehen werden können.[205] Mit dem jeweiligen EPC als „Schlüssel" lassen sich dann die Daten online abrufen.[206]

Der Code ist eine Aneinanderreihung binärer Zahlen, momentan zwischen 64 und 96 Bit lang, in der Zukunft zwischen 128 und 256 Bit.[207] Er ist aufgebaut in vier Sektionen[208], die von links nach rechts gelesen werden: *Header*, *EPC Manager*, *Object Class* und *Serial Number*.[209] Die erste Sektion enthält die Information darüber, welches EPC-Format verwendet wird. In der zweiten Sektion ist gespeichert, welches Unternehmen das RFID-Tag hergestellt bzw. an das Produkt angebracht hat. Als drittes folgt die Produktklasse des Artikels. Die letzten maximal neun Stellen des EPC ergeben eine Seriennummer, also eine einzigartige Nummer für den Artikel aus der entsprechenden Produktklasse des jeweiligen Herstellers. Gleiche Produkte aus derselben Produktion haben demnach bis auf die letzten neun Stellen denselben EPC. Die letzten neun Ziffern entscheiden über die eindeutige Identifizierbarkeit des einzelnen Gegen-

[201] Vgl. hierzu einen der Mitgründer des AutoID-Labs *Sarma*, A History oft he EPC *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 39; *Heinrich* (Hrsg.), RFID and Beyond, S. 104.

[202] *Garfinkel/Holtzman*, Understanding RFID Technology *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 22.

[203] Bereits diese Informationen sollen aber nur durch EPCglobal autorisierten Personen zur Verfügung gestellt werden, vgl. *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 101.

[204] In diesem Bereich gibt es allerdings Forschungsansätze, die statt „root"-Servern „Filterserver" einsetzten wollen. Diese leiten die Kundenanfrage direkt an die entsprechenden Herstellerserver weiter. Eine zweite Anfrage des Kunden wird damit umgangen und gleichzeitig die Daten des Herstellers nicht automatisch an den Anfragenden freigegeben. Vielmehr liegt es dann in der Hand des Herstellers, ob er auf die Anfrage mit den entsprechenden Informationen reagiert oder ob er die Anfrage schlicht ignoriert. Das so genannte "Query Relay" reduziert damit nicht nur Zeit- und Infrastrukturaufwand sondern auch potenzielle Privacy-Probleme im Bereich der Freigabe von Herstellerdaten, vgl. *Kürschner/Condea/Kasten/Thiesse*, Discovery Service Design in the EPCglobal Network *in*: Flörkemeier/Langheinrich/Fleisch/Mattern/Sarma, The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 19 ff.

[205] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 99.

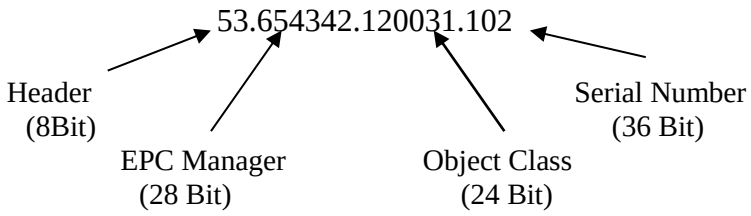
[206] *Heinrich* (Hrsg.), RFID and Beyond, S. 107.

[207] *Heinrich* (Hrsg.), RFID and Beyond, S. 104.

[208] *Heinrich* (Hrsg.), RFID and Beyond, S. 107.

[209] *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 90.

standes. Folgende Grafik zeigt den EPC im General-Identifier-Format (GID) in der 96-Bit-Version.[210]



Aufbau des EPC (Quelle: *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern (Hrsg.), Das Internet der Dinge, S. 90)

Dieser momentan standardmäßig verwendete 96-Bit-EPC bietet eindeutige Identifikationsnummern für 268 Millionen Unternehmen, 16 Millionen Produktklassen und 68 Milliarden Seriennummern in jeder Produktklasse.[211]

Zwar ist das Labeling eines Produktes mit einem Barcode viel billiger, allerdings bietet ein mit einem EPC versehenes RFID-Tag im Vergleich andere – in einigen Anwendungsfeldern wesentliche – Vorteile.[212] So ist bei der Identifikation mittels Radiowellen kein visueller Kontakt mehr zwischen Tag und Reader nötig. Radiowellen durchdringen sogar die meisten Verpackungsmaterialien. Ebenso können teilweise erheblich größere Lesereichweiten erreicht werden. Auch die Erfassung von mehreren Gegenständen gleichzeitig – sogenannte Pulkerfassung[213] – ist mit RFID möglich.

EPC ist betriebswirtschaftlich motiviert. Dies ergibt sich bereits aus der Dominanz der Konsumgüterindustrie, die sich in der Zusammensetzung der EPCglobal-Mitglieder wiederspiegelt.[214] Das *Real Time Enterprise*[215]-Konzept ist ein treibender Motor in der Weiterentwicklung und weltweiten Einführung von RFID.[216] *Real Time Enterprises* – also Echtzeitunternehmen – zielen darauf ab, Informationen so schnell wie möglich – also in Echtzeit – zu erfassen, zu organisieren und entsprechend darauf zu reagieren. RFID ist eine der bevorzugten Techniken zur Erreichung dieses Ziels.[217] Ein wesentlicher Begriff im Zusammenhang mit *Real Time Enterprise* und RFID ist *Real World Awareness*. Ganz grundsätzlich geht es hierbei

---

[210] Vgl. zum EPC im *Serialized-General-Trade-Item-Number*-Format (SGTIN), der zusätzlich zum GID noch Felder für die aus dem *Universal Product Code* sowie der EAN-Nummer stammenden Informationen zum Herstellercode und Produkttyp enthält *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. S. 90.

[211] *Heinrich* (Hrsg.), RFID and Beyond, S. 108.

[212] Vgl. *Heinrich* (Hrsg.), RFID and Beyond, S. 63 f.

[213] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 164, 174 f.; BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 25.

[214] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 30; vgl. auch schon Fn. 194, 195.

[215] Vgl. zu Real-Time Enterprises *Thielmann/Kuhlin*, Real-Time Enterprise in der Praxis.

[216] Vgl. zu RFID in Real-Time-Enterprise Systeminfrastrukturen *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 151 ff.

[217] *Thielmann/Kuhlin*, Real-Time Enterprise in der Praxis, S. 258 ff.

zunächst um jede Technik, die es ermöglicht, mit Computern in Echtzeit Gegenstände in der Realworld zu verfolgen, auf die gewonnenen Informationen angemessen zu reagieren[218] und hierbei Medienbrüche zu vermeiden.[219] Um eine derartige Verfolgbarkeit zu erreichen muss eine entsprechende Infrastruktur eingerichtet werden, sprich die Objekte müssen mit maschinenlesbaren Tags ausgerüstet und an den strategisch wichtigen Punkten damit kompatible Reader installiert werden. Diese allgegenwärtige Informatisierung der Umwelt wird auch als *Ubiquitous Computing* oder *Pervasive Computing*[220] beschrieben.[221]

Das Ziel der Erfinder von EPC, dem AutoID-Team, war die Erschaffung eines „Internet der Dinge".[222] In Zukunft sollen nicht nur Computer miteinander vernetzt sein. Jeder Gegenstand, der neu produziert wird, soll bereits während des Herstellungsprozesses mit einem RFID-Tag ausgestattet werden. Ältere Gegenstände können nachgerüstet werden. Alle getaggten Gegenstände können dann miteinander oder mit Computersystemen weltweit kommunizieren.[223] Alltägliche Gegenstände werden damit zu *smart things*, Gegenständen, die „wissen", wo sie sich befinden, welche anderen Gegenstände in der Nähe sind und mit deren EPC in Datenbanken weitergehende Informationen über sie gespeichert werden, die dann von jeder (autorisierten) Person mit einem Reader nachvollzogen werden können.

Neben dem global einsetzbaren EPC erarbeitet EPCglobal zudem Standards für die Kommunikation zwischen Tag und Reader, für die Datenübertragung zwischen Reader und Hintergrundsystem, Reader- und Luftschnittstellenprotokolle, sowie weitere Standards für die RFID Infrastruktur.[224] Um die riesige Menge in RFID-Systemen anfallender Daten zu organisieren wurde beispielsweise die als *Middleware* fungierende Software Savant entwickelt, die Lesegeräte steuern und Anwendungen mit entsprechend aufbereiteten Daten versorgen kann.[225]

Ein „Internet der Dinge" hätte vielfältigste Vorteile. In der Produktlieferkette aber auch im Alltag eines jeden Menschen sind Vereinfachungen und Effizienzsteigerungen denkbar. Ob es das oben dargestellte Regal im Supermarkt ist, das erkennt, dass nur noch zwei Packungen des Orangensaftes der Marke X vorhanden sind und dies im Lager meldet oder der intelligente Kühlschrank zu Hause, der warnt, dass die Milch abgelaufen ist. Generell geht es darum,

---

[218] *Heinrich* (Hrsg.), RFID and Beyond, S. 61.

[219] *Thielmann/Kuhlin*, Real-Time Enterprise in der Praxis, S. 33.

[220] „Ubiquitous" bedeutet allgegenwärtig, „pervasive" hingegen durchdringend.

[221] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 30.

[222] *Heinrich* (Hrsg.), RFID and Beyond, S. 104.

[223] *Heinrich* (Hrsg.), RFID and Beyond, S. 56.

[224] Vgl. für eine Übersicht über die verschiedenen Standards (Stand 2005) *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 101 f.; BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 18 ff.

[225] *Flörkemeier*, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in*: Fleisch/Mattern, (Hrsg.), Das Internet der Dinge, S. 88, 94. Standard ist *Savant* allerdings nicht einmal im EPCglobal-Network geworden. Vielmehr hat sich das Unternehmen darauf beschränkt die Schnittstelle zwischen Middleware und Anwendungssoftware zu normieren. Die Ausgestaltung der Middleware bleibt damit den jeweiligen Herstellern und Verwendern der RFID Systeme überlassen, vgl. BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 35.

die Lücke zwischen Realworld und Cyberworld zu schließen und damit (Geschäfts-)Abläufe zu verbessern.[226]

Auf dem Weg zu einem „Internet der Dinge“ ist EPC bzw. Standardisierung der unverzichtbare Faktor.[227] Ebenso wenig wie ein Internet der Computer ohne einzigartige IP-Adresse eines jeden Rechners denkbar ist, ist auch ein Internet der Dinge ohne eindeutige Identifikationsnummern auf jedem einzelnen Gegenstand nicht praktikabel. EPC soll in dieser Arbeit zunächst vereinfachend für jedes RFID-System mit eindeutigen Identifikationsnummern auf dem Tag stehen. Zwar ist zu erwarten, dass sich auf lange Sicht ein oder jedenfalls nur wenige Systeme als globaler, mindestens internationaler Standard herausbilden. Zum jetzigen Zeitpunkt ist eine solch flächendeckende Standardisierung aber unter anderem aus den oben erläuterten technischen Gründen[228] noch nicht erfolgt. Vor diesem Hintergrund erklärt sich auch die oben angesprochene teilweise Unterteilung in offene und geschlossene Systeme[229]. Hier soll aber davon ausgegangen werden, dass RFID-Systeme in der Zukunft tatsächlich ubiquitär, weil umfassend standardisiert, sein werden.

In der Praxis ergeben sich mit den erläuterten betriebswirtschaftlichen Hintergründen **vier** zeitlich und räumlich zu unterscheidende Unterfälle der Anwendung von RFID in der Lieferkette.

(a) Phase 1 betrifft die Phase der Herstellung des Produkts und seine Etikettierung mit einem RFID-Tag bis zur Ankunft im Lager des Einzelhändlers – *Herstellungsphase.*

(b) Phase 2 beschreibt die Phase, in der das Produkt auf der Verkaufsfläche für den Kunden zugänglich gemacht wird – *Verkaufsphase.*

(c) Phase 3 ist die Phase nach dem Kauf des Produkts durch den Kunden und dessen Verlassen des Ladens mit dem getaggten Produkt – *Nutzungsphase.*

(d) Phase 4 betrifft zuletzt den Zeitraum, in dem sich der Kunde bereits des Produktes entledigt hat und es der Kreislaufwirtschaft zugeführt wird – *Recyclingphase.*

a) Herstellungsphase

Die Vorzüge von RFID in der Herstellungs- und Lieferkette sind nur dann optimal zu nutzen, wenn das Produkt unmittelbar nach seiner Herstellung oder sogar schon während dessen getaggt wird. Dann nämlich lässt sich eine Verfolgung in Echtzeit bereits in der Produktionshalle durchführen. Produktionslinien können damit voll ausgelastet und folglich eine größtmögliche Produktionszahl erreicht werden. Nach der Produktion folgt die Distribution des Produktes. In den meisten Fällen werden zunächst Zwischenhändler mit dem Produkt beliefert. Auch im Rahmen dieses Verteilungsprozess lassen sich mit RFID im Vergleich zu herkömmlichen

---

[226] *Heinrich* (Hrsg.), RFID and Beyond, S. 56.

[227] So auch *Heinrich* (Hrsg.), RFID and Beyond, S. 67, der sogar den Erfolg von RFID generell abhängig von einem einheitlichen Identifikationsschema sieht; zu Standardisierungsfragen auch *Huber*, MMR 2006, 728 (731).

[228] Vgl. zu den Frequenzen B.I.2.b)aa).

[229] Vgl. B.II.1.

Identifikationssystemen Effizienzsteigerungen herbeiführen. Die ausliefernden Lkw können ohne Zeitverlust genau geordert werden, die Erfassung der Produkte beim (Zwischen)Händler erfolgt in Echtzeit also ohne Zeitverlust. Dies ist möglich, indem neue und vom System des Händlers zu erfassende Produkte – im Pulk – nur noch durch eine „Leseschranke“[230] hindurchgeführt werden müssen. Die Erfassung aller einzelnen Produkte kann dann über das Einlesen der auf den Tags gespeicherten Informationen erfolgen. Ein Einscannen oder gar manuelles Aufnehmen ins System entfällt. Nicht nur die Zeitersparnis beim Erfassen der neuen Waren ist ein wichtiger Aspekt, sondern insbesondere auch die Überprüfung der Vollständigkeit der Lieferung. Kann bei mit Barcodes versehen Palletten nicht bzw. nur mit enormem Aufwand überprüft werden, ob auch die vollständige Zahl an Einzelprodukten darauf enthalten ist, ermöglicht RFID die Erfassung aller Produkte in wesentlich viel kürzerer Zeit. Auch die Organisation der Waren im Lager des Händlers lässt sich mittels RFID vereinfachen. Örtlich angebrachte Lesegeräte können immer genauen Aufschluss darüber geben, welche Waren sich wo im Lager befinden. Die Suche nach einer bestimmten Palette entfällt damit ebenfalls.

In der gesamten Zeit der Produktion bis zur Ankunft des Produkts im Lager des Händlers kommt der Endkunde nicht mit dem RFID-Tag in Kontakt. Lediglich logistische Abläufe werden damit verbessert. Datenschutzherausforderungen ergeben sich damit jedenfalls nicht im Endkundenbereich. Denkbar ist aber eine möglicherweise arbeitsrechtlich zu berücksichtigende Gefährdung der Privatheit der Angestellten (Lagerarbeiter, Lkw-Fahrer etc.), die indes – wie bereits oben dargelegt – nicht Gegenstand dieser Arbeit sein soll.

b) Verkaufsphase

Dies ändert sich ab dem Moment, in dem das Produkt auf der Verkaufsfläche des Händlers für den Kunden zugänglich gemacht wird. Auch hier spielen natürlich weiterhin logistische Aspekte eine Rolle. Inventuren werden massiv vereinfacht, das Auffinden eines bestimmten Artikels mittels mobiler Lesegeräte ist möglich. Sobald aber der Kunde ein Produkt an sich nimmt treten aus rechtlicher Sicht ganz andere Gesichtspunkte in den Vordergrund. Entscheidet sich der Kunde für das Produkt, trägt er es den Rest seines Aufenthalts in den Geschäftsräumen mit sich herum bzw. fährt es mit dem Einkaufswagen durch den Laden. Dies macht es für den Einzelhändler interessant, punktuell an strategischen Orten oder auch in den Einkaufswagen Lesegeräte zu installieren. Ein Grund hierfür ist die Schaltung kundensensitiver Werbung und die Erstellung von Bewegungs- bzw. sogar personalisierten Kunden- und Verhaltensprofilen.

c) Nutzungsphase

Die Nutzungsphase beginnt in dem Moment, in dem der Kunde mit dem bezahlten aber weiterhin getaggten Produkt den Laden verlässt. Nicht betroffen von diesem Szenario ist man also nur dann, wenn das RFID-Tag an der Kasse entfernt oder zerstört wird. Bleibt das Tag hingegen aktiv trägt der Kunde zumindest bis nach Hause zusätzlich zu dem von ihm zu nut-

[230] Auch „Gate Reader“ genannt, vgl. BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 26.

zenden Produkt einen Sender mit sich herum, der in Reichweite eines Lesegerätes seine – wenn auch im Regelfall nur sehr beschränkten – Daten übermittelt.

Eine entsprechende RFID-Infrastruktur vorausgesetzt, kann der Weg des Produktes sogar außerhalb der Geschäftsräume des Einzelhändlers, der das getaggte Produkt verkauft hat, verfolgt werden – und mit ihm die Person, die es gekauft hat und bei sich trägt. Bei Lebensmitteln und sonstigen Einwegprodukten könnte entsprechend nur ein Weg aufgezeichnet werden – regelmäßig vom Laden zum Kunden nach Hause. Bei Alltagsgegenständen hingegen, die man regelmäßig oder immer bei sich trägt, wie beispielsweise dem Handy oder dem Portemonnaie, könnten ganze Muster vom Verbleib und der Bewegung des Artikels erstellt werden. Immer, wenn der Artikel mit seiner einzigartigen Identifikationsnummer an einem bestimmten Lesegerät vorbeikommt, kann ein Vermerk hierüber angefertigt werden. Mit der Zeit lassen sich dadurch Bewegungs-, Verhaltens- und womöglich sogar Persönlichkeitsmuster der das Produkt bei sich führenden Person erstellen, ohne dass diese dafür identifiziert werden müsste.

d) Recyclingphase

RFID auf Produktebene kann sogar noch Verwendung finden, wenn das Produkt bereits vom Kunden entsorgt wurde. Auch in der Kreislaufwirtschaft lässt sich RFID sinnvoll einsetzen.[231] So kann auf dem Tag oder im Hintergrundsystem die Zusammensetzung des jeweiligen Produktes gespeichert und damit automatisch die richtige Verwertungsform gefunden werden. Auf diese Weise kann der Recyclingvorgang nicht nur effizienter sondern auch umweltverträglicher gemacht werden. Weiterhin ließe sich das im Umwelt- und Kreislaufwirtschafts- und Abfallrecht geltende Verursacherprinzip besser durchsetzen. Durch die Speicherung der Kundendaten mit den Produktdaten könnte – dies erlaubende gesetzliche Regelungen vorausgesetzt – nachträglich ermittelt werden, wer der Verursacher des Abfalls ist.

2. RTAMP

Neben EPC ist RTAMP das für die Datenschutzdebatte zweite wichtige Szenario. RTAMP steht für *Real Time Authentication and Monitoring of Persons*. Gemeint ist die Möglichkeit der Echtzeit-Authentifizierung und -verfolgung genau identifizierter Personen. Die Lokalisierung von Menschen funktioniert bereits heute beispielsweise über *Global Positioning* Systeme (GPS)[232]. Mit der Möglichkeit der Implantierung von RFID-Tags unter die Haut ergibt sich allerdings eine neue Qualität dieser Ortungs- und Verfolgungsmöglichkeit. Unterschieden werden muss zwischen implantierten RFID-Tags auf der einen und dauerhaft bei sich zu tragenden Tags bzw. getaggten Gegenständen auf der anderen Seite. Zunächst ist ein Tracking mittels unter die Haut oder anderweitig implantierter RFID-Chips denkbar. Aber auch über das regelmäßige Beisichführen von Gegenständen, die getaggt sind und auf deren Tags entweder unmittelbar oder zumindest in der verbundenen Datenbank personenbezogene Daten

[231] Vgl. hierzu *Roßnagel/Hornung*, UPR 2007, 255 ff.

[232] Vgl. zur Funktionsweise und zu den Anwendungsbereichen von GPS *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 172 ff.

gespeichert sind, können genau identifizierte Personen überwacht werden. In beiden Fällen ist RFID mehr oder weniger allgegenwärtig, also ubiquitär. Entsprechend kann im ersten Fall von *intrinsic ubiquity* und im zweiten von *extrinsic ubiquity* gesprochen werden.[233]

3. RTAMA

RTAMA steht für *Real Time Authentication and Monitoring of Animals*. Auch Tiere können natürlich mit einem RFID-Chip "getaggt" werden. In Betracht kommt dies zum einen bei Nutztieren (Schlachtvieh) aber auch Haustieren.

4. AGG

Zuletzt sind neben der isolierten Betrachtung der drei vorangegangenen Szenarien auch Situationen denkbar, in denen die für den jeweiligen Szenario-Typ erforderlichen mit anderen Daten kombiniert werden, sog. *Aggregationsszenarien* (AGG). Für diese Arbeit relevant ist dabei insbesondere die Verbindung von EPC und personenbezogenen (Kunden-)Daten.

II. Herausforderungen

Gerade aufgrund der kontaktlosen Auslesbarkeit ergeben sich im Bereich von RFID-Systemen neue Sicherheitsrisiken für die Technik als solche und die betroffenen Daten im Speziellen. Identifikationssysteme sind ohne die Gewährleistung der Integrität sowie der Verfügbarkeit des Systems und der Daten wertlos.

1. Tracking

Die Verwendung von RFID-Tags zur Zugangs- und Aufenthaltskontrolle in Unternehmen eröffnet dem Arbeitgeber als Verwender des Systems weitere für ihn möglicherweise interessante Anwendungsbereiche. Denkbar ist zum Beispiel einem bestimmten Angestellten nur einen bestimmten Weg zu seinem Arbeitsplatz zu öffnen, ihn also auf einer vorher festgelegten Route durch das Gebäude zu leiten. Auch der Zugang zu bestimmten Bereichen wie der Kantine könnte zeitlich reglementiert werden.[234] Es ergibt sich die Möglichkeit der Verfolgung der Mitarbeiter im Gebäude in Echtzeit und die Speicherung der jeweiligen Aufenthaltsorte mit Zeitangabe.[235] So hat sich die amerikanische Videoüberwachungsfirma CityWatcher im Februar 2006 dazu entschlossen, ihren Mitarbeitern RFID-Chips der Marke VeriChip zu implantieren, um die Zutrittskontrolle für Kontrollräume zu verbessern.[236]

---

[233] Zu den Begriffen der *intrinsic* sowie *extrinsic ubiquity* vgl. schon *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 205.

[234] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 20.

[235] Vgl. auch *Balkovic/Bikson/Bitko*, 9 to 5: "Do You Know If Your Boss Knows Where You Are?" Case Studies of Radio Frequency Identification Usage in the Workplace, abrufbar unter http://www.rand.org/pubs/technical_reports/2005/RAND_TR197.pdf (04.04.2013).

[236] Heise News Meldung vom 10.02.2006, Firma markiert Mitarbeiter per RFID, abrufbar unter http://www.heise.de/newsticker/meldung/69438/ (04.04.2013).

Die Tracking-Funktion kann in gefährlichen Arbeitsumgebungen zum Sicherheitsaspekt werden und für lebensrettende Maßnahmen eingesetzt werden. Immer wieder bekannt werdende Mienenunglücke, bei denen Kumpel unter der Erde eingeschlossen werden und oft nicht einmal ihr genauer Standpunkt bekannt ist, geben Anlass zu der Überlegung RFID in diesem Bereich zu verwenden.[237]

Auch in Hochsicherheitsumgebungen – wie Gefängnissen – ist die Verwendung RFID gestützter Systeme denkbar. In einer U.S. amerikanischen Gesetzgebungsinitiative im Staat Texas ist dieser Gedanke bereits aufgegriffen worden. [238] So hätten nach der Initiative alle Inhaftierten aber auch Besucher, Personal und sonstige Personen in der Zeit ihres Aufenthaltes ein RFID-Tag bei sich tragen müssen, um eine ständige Auffindbarkeit und Verfolgbarkeit gewährleisten zu können. Im niederländischen Gefängnis Lelystad – eine extra zum Test von RFID gebaute Institution – bekamen 150 freiwillige Insassen nicht entfernbare RFID getaggte Armbänder. Die betreffenden Straftäter wurden in Echtzeit verfolgt. Ziel war es neue Haftkonzepte zu erarbeiten.[239]

Im deutschen Recht findet sich zur Verwendung von RFID in Strafvollzugsanstalten eine Regelung im baden-württembergischen Justizvollzugsgeetzbuch.[240] Dieses sieht die Verwendung von RFID zur Identifikation und Lokalisierung von Strafgefangenen vor, setzt aber die Einwilligung des Gefangenen voraus, vgl. 33 JVollzGB BW:

> § 33 JVollzGB Datenerhebung durch Radio-Frequenz-Identifikation (RFID)
>
> (1) Aus Gründen der Sicherheit oder Ordnung der Justizvollzugsanstalt oder zur Überwachung des Aufenthaltsorts von Gefangenen auf dem Anstaltsgelände kann die Justizvollzugsanstalt Daten über den Aufenthaltsort und den Zeitpunkt der Datenerhebung mittels RFID-Transponder durch Empfangsgeräte automatisiert erheben.
>
> (2) Mit Einwilligung der oder des Gefangenen kann ein RFID-Transponder zur automatisierten Identifikation und Lokalisierung so mit ihrem oder seinem Körper verbunden werden, dass eine ordnungsgemäße Trennung nur durch die Justizvollzugsanstalt erfolgen kann. Von der Einwilligung können die Rücknahme besonderer Sicherungsmaßnahmen oder die Einteilung der oder des Gefangenen zu einer in bestimmten Bereichen auf dem Anstaltsgelände zu leistenden Arbeit abhängig gemacht werden.

In Japan geht man noch einen Schritt weiter. In einer japanischen Schule wurden den Schulkindern RFID-Tags ausgehändigt, die diese dauerhaft an ihrem Rucksack tragen mussten, nachdem 2001 acht Kinder auf dem Schulhof von einem Mann erstochen und dreizehn weite-

---

[237] RFID Journal, Meldung vom 19.06.2006, Active RFID Drills into Mining Industrie, abrufbar unter http://www.rfidjournal.com/article/view/6517 (04.04.2013); Sensors, Meldung vom 01.02.2004, When Safety Matters: Using Active RFID Down in the Mines, abrufbar unter http://www.sensorsmag.com/sensors/article/articleDetail.jsp?id=319650 (04.04.2013); vgl. auch die Verwendung von RFID beim Bau des neuen Gotthard-Tunnels in der Schweiz zur Ortung der Bauarbeiter im Unglücksfall, *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 229.

[238] Texas H.B. 2990, 2007. Dieser Gesetzentwurf ist allerdings nach einem Veto von Governor Perry nicht in Kraft getreten, vgl. die Veto-Message http://www.lrl.state.tx.us/scanned/vetoes/80/hb2990.pdf#navpanes=0 (04.04.2013).

[239] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 23.

[240] Gesetzbuch über den Justizvollzug in Baden-Württemberg (Justizvollzugsgesetzbuch – JVollzGB) vom 10. November 2009, GBl. 2009, 545, abrufbar unter http://www.landesrecht-bw.de/jportal/portal/t/aew/page/bsbawueprod.psml?showdoccase=1&doc.id=jlr-JVollzGBBW2009rahmen%3Ajuris-lr00&doc.part=X#jlr-JVollzGBBW2009pBuch1-P33 (04.04.2013).

re sowie zwei Lehrer verletzt worden waren.[241] Mittels des Tags wird die Anwesenheit der Kinder beim Passieren spezieller Lesegeräte überprüft.[242] Auch eine britische Schule testet pilotweise den Einsatz von RFID bei ihren Schülern.[243] Die RFID-Tags werden in die Schuluniformen der Schüler eingenäht. Eltern haben die Möglichkeit sich mittels internetfähigen Endgeräts genau anzeigen zu lassen, in welchem Raum in der Schule sich ihr Kind gerade aufhält. Haben sich die Kinder nicht ordnungsgemäß in der Schule gemeldet, bekommen die Eltern automatisch eine Benachrichtigung auf ihr Handy oder per E-Mail. Die RFID-Tags können auch zur Zugangskontrolle genutzt werden. Nach eigenen Angaben können die Tags „nur" aus bis zu zwei Metern Entfernung ausgelesen werden. Auch im LEGOland in Billund, Dänemark wurde ein ähnliches System eingeführt.[244] Nachdem jährlich ca. 1600 Kinder „abhanden" kamen, wurde der Kidspotter installiert. Ein System, bei dem die Eltern beim Betreten des Unterhaltungsparks ein RFID-Armband für ihr Kind mieten können, durch das dann wiederum das Auffinden des Kindes an jedem Punkt im Park möglich ist. Die Eltern können sich den Aufenthaltsort dann per SMS auf ihr Handy schicken lassen.

Wie bereits oben angesprochen kann RFID auch im Gesundheitswesen Verwendung finden. Getaggt werden können nicht nur Inventar oder Operationsinstrumente. Auch die Patienten könnten „getaggt" werden, beispielsweise indem sie bei der Aufnahme ein RFID-Armband umgebunden bekommen, auf dem dann entweder direkt oder in Verbindung mit einem Hintergrundsystem ihre medizinischen Daten gespeichert sind.[245] Die Patienten hätten damit immer ihre elektronische Krankenakte dabei. Daneben könnte mit einem solchen Armband auch wieder die Anwesenheit der Patienten überprüft und ihre Bewegungen in der Klinik verfolgt werden. Außer in Krankenhäusern können auch in Pflege- und sonstigen Betreuungseinrichtungen die Bewohner mit RFID ausgerüstet werden. Das Betreuungsrecht stellt hier eigene Anforderungen, die – wie eingangs bereits erklärt – in dieser Arbeit nicht behandelt werden.[246]

Der Kopenhagener Flughafen hat Anfang 2008 ein Pilotprojekt gestartet, bei dem Flugpassagiere beim Check-In ein aktives RFID-Tag ausgehändigt bekommen, mithilfe dessen sie

---

[241] CBS News vom 11.10.2004, Japanese Kids get Radio ID'd, abrufbar unter http://www.cbsnews.com/stories/2004/10/11/tech/main648681.shtml (04.04.2013).

[242] *Heinrich* (Hrsg.), RFID and Beyond, S. 178.

[243] Heise News Meldung vom 21.10.2007, Britische Schule testet RFID-Chips in der Schulkleidung, abrufbar unter http://www.heise.de/newsticker/meldung/97700 (04.04.2013).

[244] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 15.

[245] So wurde es bei einem Pilot-Projekt im New Yorker Jacobi Medical Center auch getan, vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 72; auch im Klinikum Saarbrücken bekommen Patienten ein RFID Armband umgebunden, auf dem eine Patientennummer gespeichert ist, vgl. Deutscher Bundestag, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie, oben Fn. 43, S. 6.

[246] Zum Einsatz von RFID in Betreuungssituationen sind bereits mehrere Urteile ergangen, vgl. etwa OLG Brandenburg, Beschl. v. 19.01.2006, FamRZ 2006, 1481, LG Ulm Beschl. v. 25.06.2008, NJW-RR 2009, 225, s. auch *Kreicker*, NJW 2009, 890.

während ihres Aufenthalts im Flughafen geortet – also ihre Bewegungen „getrackt“ – werden und sie gewarnt werden können, wenn sie sich trotz bevorstehenden Boardings noch weit entfernt von ihrem Abfluggate befinden.[247] Hintergrund ist die Reduzierung von Flugverspätungen aufgrund von zu spät am Gate ankommenden Passagieren und die Aufzeichnung von Passagierströmen innerhalb des Flughafengeländes.[248] Das System funktioniert dergestalt, dass durch ein Zusammenspiel des RFID-Systems und dem Handy des jeweiligen Passagiers zunächst dessen Aufenthaltsort bestimmt und ihm dann im Zweifel eine Warn-SMS auf sein Handy geschickt wird. Die RFID-Tags geben die Passagiere beim Boarden wieder an die Bodencrew zurück. Da es sich hierbei bis jetzt nur um ein Pilot-Projekt handelt, gibt es noch keine Informationen, ob der Flughafenbetreiber eine mögliche Opt-Out-Regelung vorsieht, die Passagiere also die Annahme des RFID-Tags verweigern dürfen.

Auch im Zusammenhang mit RFID getaggten ÖPNV-Tickets ist ein Tracking der Fahrgäste denkbar. Aufsehenerregend bei der Londoner Oyster Card war aber nicht die bloße Möglichkeit des Trackings von Personen, sondern dass es tatsächlich stattfand: Die Londoner Polizei stellte seit der Einführung der Oyster Card mehrere Anfragen bezüglich der Kunden- und damit Bewegungsdaten mehrerer Fahrgäste.[249] Hintergrund war die Aufklärung verschiedener Straftaten.[250] Das ÖPNV-Unternehmen Transport for London verteidigte sich und versicherte, dass die Fahrgastdaten nicht zum Zwecke des Tracking sondern zur Verbesserung des Kundenservice erhoben würden.[251]

Auch mittels unter die Haut implantierter Tags wie dem VeriChip ist ein Tracking der Träger in Echtzeit möglich. Ob und inwieweit dann womöglich auf die gespeicherten Daten im Hintergrundsystem zurückgegriffen werden kann, ist eine Frage der Regelung der Zugriffsberechtigung und Sicherung des Systems gegen unbefugtes Eindringen. Betritt ein VeriChip-Träger einen Supermarkt, erfasst der Reader an der Tür lediglich die auf dem Chip gespeicherte Identifikationsnummer. Ist das Hintergrundsystem entsprechend gesichert, kann der Supermarktbetreiber dann keine weiteren Informationen gewinnen. Ein Tracking des Trägers bleibt aber aufgrund der eindeutigen Nummer möglich.

Die hier aufgeführten Möglichkeiten des Tracking verdeutlichen zunächst die Vorteile, die mittels RFID-Technik zur Steigerung von Sicherheit und Effizienz erzielt werden können. Diese sind indes nur die eine Seite der Medaille: Das entstehende Überwachungspotenzial kann auch zu persönlichkeitsrechtsgefährdenden Maßnahmen verwendet werden. Das Anle-

---

[247] RFID Journal News, Meldung vom 30.05.2008, Copenhagen Airport Pilots RFID-Tags for Passengers, abrufbar unter http://www.rfidjournal.com/article/articleview/4104/1/1/ (04.04.2013).

[248] Vgl. auch die Informationen auf der Homepage des Flughafens, http://www.cph.dk/cph/uk/newsroom/news/2008/wireless+technology.htm (04.04.2013).

[249] Alleine im Januar 2006 wurden 61 solcher Anfragen durch TfL erfüllt. Vgl. Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 12.

[250] Vgl. BBC News vom 13.03.2006, Oyster data is 'new police tool', abrufbar unter http://news.bbc.co.uk/1/hi/england/london/4800490.stm (04.04.2013).

[251] Die ursprünglich unter http://www.tfl.gov.uk/assets/downloads/foi/Request_directory_06_-_Oyster_data_sharing.pdf (letzter Abruf 08.10.2007) abrufbare Antwort auf eine besorgte Kundenanfrage ist mittlerweile nicht mehr abrufbar.

gen umfassender Verhaltens-, Bewegungs- und sogar Persönlichkeitsprofile (hierzu sogleich mehr) oder die Totalüberwachung der Betroffenen wird möglich.

Zwar besteht diese Möglichkeit auch bereits durch andere Techniken, wie z.B. die GPS-Funktion im Mobiltelefon, indes liegt es bei diesen Techniken regelmäßig in der Hand des Betroffenen, sie ein- oder eben auch auszuschalten. In einer ubiquitären RFID-Umgebung entfällt diese Möglichkeit.

2. Profilbildung

Gerade im Einzelhandel soll sich die Möglichkeit des RFID-gestützten Tracking und Tracing vorteilhaft für Unternehmen auswirken. Verfolgt und gespeichert werden kann zunächst der Weg der Produkte durch den Laden. Mit den Produkten können gleichzeitig die sie bei sich führenden Kunden verfolgt werden. Durch Organisation der gesammelten Daten lassen sich Profile erstellen. Die Nutzung der gewonnenen Bewegungsdaten zur Erstellung von Verhaltungs- und womöglich sogar personalisierten Kundenprofilen ist also die Weiterführung des bloßen Tracking und Tracing. Hierbei ist zunächst zwischen zwei Gruppen von Profilen zu unterscheiden. Es ist einerseits die Profilierung des unbekannten – also nicht anhand konventioneller Identifikationsmerkmale identifizierten – Kunden möglich (Pseudo-Analyse, Pseudo-Werbung) sowie andererseits die Profilierung des – namentlich oder mittels anderer Merkmale – bekannten Kunden (Individual-Analyse, Individual-Werbung). Ad-hoc-Werbung, dem momentanen Kundenverhalten angepasst und damit auch ohne vorherige Erstellung eines Profils möglich, ist den beiden Gruppen vorgelagert.[252]

Solche Bewegungsprofile betreffen den Bereich der *Location Privacy*[253], also die Bestimmung des Aufenthaltsorts des Betroffenen und seiner Bewegungen. Hierbei gilt: Je mehr Tags im Umlauf sind und der Betroffene bei sich führt, desto größer sind die Möglichkeiten im Wege der Verknüpfung der verschiedenen Tag-Daten, dezidierte Profile anzulegen. Denn: Während ein einzelner Gegenstand mit recht hoher Wahrscheinlichkeit im Laufe seines Bestehens den Besitzer wechseln wird (z.B. NUR das Portemonnaie), ist es wesentlich unwahrscheinlicher, dass eine ganze Anzahl an Gegenständen dies tut (das Portemonnaie UND die Brille UND die Schuhe). Durch Zusammenführung der einzelnen Tag-Daten von Portemonnaie, Brille und Schuhen kann mit großer Sicherheit darauf geschlossen werden, dass es sich um ein und denselben Betroffenen handelt.

---

[252] Vgl. zu dieser Einteilung bereits *Flörkemeier/Schneider/Langheinrich*, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols *in*: Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda, Michiaki Yasumura (Hrsg.), Ubiquitious Computing Systems; Revised Selected Papers from the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan, Lecture Notes in Computer Science, Vol. 3598 S. 6, abrufbar unter http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf (04.04.2013).

[253] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 47.

a) Ad-hoc-Werbung

Ad-hoc-Werbung[254] beschreibt den Vorgang, bei dem der Kunde auf sein momentanes Verhalten maßgeschneiderte Werbung unterbreitet bekommt. Erkennt ein Smart-Shelve in einem Kaufhaus beispielsweise, dass eine Kundin oder ein Kunde ein blaues Polo-Shirt der Marke Z von der Stange genommen hat und nun mit sich herumträgt, können auf entsprechend positionierten Bildschirmen Vorschläge für zu dem Shirt passende Accessoires unterbreitet werden. Für diesen Vorgang ist eine vorherige Erstellung eines Kundenprofiles nicht erforderlich. Es reichen die in Echtzeit gewonnenen Informationen aus.

b) Pseudo-Analyse

Analysiert und organisiert der Verwender des RFID Systems allerdings die gewonnenen Daten, kann er Profile erstellen. Die Vorteile dieser Kundenprofilierung sind vielfältig. Der Einzelhändler, der weiß, wo sich die Kunden verstärkt aufhalten, kann entsprechende Positionierungsstrategien für die Produkte entwickeln.[255]

Ein Praxisbeispiel für die Pseudo-Analyse[256], bei dem es sich allerdings nicht um einen Supermarkt handelt, ist der Zoo von Apenheul[257]. Hier werden beim Betreten des Zoogeländes RFID getaggte Tüten an die Besucher verteilt.

> „The Apenheul […] is a zoo specialized in all kinds of apes and monkeys. An outstanding feature of the park is the opportunity for some kinds of monkeys to move freely through the crowd of visitors. Curious as they are, the monkeys often try to open visitors' bags in hope of a free lunch. The park therefore introduced the "Monkey bag", a green bag with an extra clip lock which monkeys cannot open. The bag is obligatory, which is enforced by the receptionists providing the bag at the entrance of the park and a warning sign. Aside from this security reason for implementing the bag, the department of marketing added a marketing feature to the bag: scanning visitors' movements through the park through an active RFID sewn into the bag."[258]

Die Zoobesucher, die eine solche Tüte ausgehändigt bekommen haben, wurden nicht auf das RFID-Tag hingewiesen.[259] Begründet wurde dies damit, dass keinerlei personenbezogene Daten gesammelt oder verarbeitet würden. Eine namentlich nicht identifizierte Person trägt also ein RFID-Tag mit sich herum, wodurch Bewegungsprofile erstellt werden können. Der Zoobesitzer kann mit den gewonnenen Informationen wiederum Rückschlüsse auf die Interessen der Besucher ziehen und sein Angebot daran ausrichten.

---

[254] Vgl. hierzu *Flörkemeier/Schneider/Langheinrich*, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, oben Fn. 252, S. 6.

[255] Vgl. *Langheinrich*, Gibt es in einer total informatisierten Welt noch eine Privatsphäre? *in*: Mattern (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, S. 237, oben Fn. 120, der auf ein Pilotprojekt in 69 Samsung-Tesco-Supermärkten in Korea verweist.

[256] Vgl. hierzu *Flörkemeier/Schneider/Langheinrich*, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, oben Fn. 252, S. 6.

[257] S. hierzu schon *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 197 f.

[258] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 16.

[259] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 16.

In gleicher Weise wie der Besitzer des Zoos von Apenheul die Besucher anhand der RFID-Tüte verfolgen kann, kann auch der Supermarktbesitzer anhand der Bewegung der getaggten Produkte und Einkaufswagen im Laden den Weg der Kunden nachverfolgen.

Werden die Tags nach dem Verlassen der Einrichtung – sei es Supermarkt oder Zoo – vernichtet oder entfernt, ist eine weitergehende Verfolgung des Kunden mittels dieser Tags unmöglich. Bleiben die Tags auf den gekauften Produkten allerdings auch nach dem Bezahlen und Verlassen des Ladens aktiv, ist ein Tracking auch außerhalb des begrenzten Raums der Ladenfläche möglich.

Das Anfertigen von Kundenprofilen ist in gewissen Konstellationen auch möglich, ohne dass der Kunde überhaupt ein Produkt ergreift oder es gar bezahlt und mit nach Hause nimmt. Hierunter fallen alle Konstellationen, in denen der betreffende Kunde bereits über eine Identifizierungsnummer bekannt ist, sprich in allen Fällen, in denen ein Chip implantiert ist oder aber ein getaggter Gegenstand regelmäßig mitgeführt wird (Portemonnaie, Brille, Schuhe).

Bei den beiden letztgenannten Beispielen ist die Erstellung von Profilen zeitlich uneingeschränkt. Solange der Kunde die Identifizierungsnummer im Chip oder Tag bei sich führt, kann der Betreiber des betreffenden RFID-Systems mit der entsprechenden Identifikationsnummer als Schlüssel zur entsprechenden Person Profile anlegen. Dies kann, ohne dass der Betreiber jemals den Namen des Kunden erfährt, zu andauernden Profilierungen führen.

c) Pseudo-Werbung

Anhand der gewonnenen Pseudo-Kundenprofile kann in einem weiteren Schritt für den jeweiligen namentlich unbekannten Kunden maßgeschneiderte Werbung[260] bereitgestellt werden. Im Unterschied zur Ad-hoc-Werbung ist dies nur in den oben letztgenannten beiden Fällen denkbar. Mittels über lange Zeiträume erstellter Profile können immer speziellere Werbekonzepte ausgearbeitet werden, sodass bereits fast eine Individual-Werbung vorliegt. Der Unterschied liegt lediglich darin, dass der Systembetreiber den Namen des Kunden nicht kennt.

d) Individual-Analyse

Die Steigerung der Pseudo-Analyse ist die Profilierung eines namentlich oder anderweitig eindeutig identifizierten Kunden. Mittels dieser Individual-Analyse[261] lässt sich das Pseudo-Kundenverhalten weiter spezifizieren. So kann der Systembetreiber nachvollziehen, wie das Verhalten von Kunden verschiedenen Alters, Geschlechts, sozialer Situation oder ähnlicher Unterscheidungsmerkmale geartet ist. Voraussetzung ist – im Unterschied zur Pseudo-Analyse, die wie oben gesehen aufgrund der eindeutigen Identifizierungsnummer ja bereits sehr individuell ist – die Identifizierung des Kunden über weitergehende Merkmale. Dies ist denkbar mittels RFID getaggter Kundenkarten, auf denen entweder direkt oder in der Daten-

[260] Vgl. hierzu *Flörkemeier/Schneider/Langheinrich*, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, oben Fn. 252, S. 6.

[261] Vgl. hierzu *Flörkemeier/Schneider/Langheinrich*, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, oben Fn. 252, S. 6.

bank der Name, möglicherweise das Alter, die Anschrift, vielleicht sogar Kreditkartendaten der Kunden gespeichert sind.

METRO gab in einer Aktion getaggte Kundenkarten an die Kunden aus. Die Karten sollten wie oben bereits angesprochen unter anderem in der Videoabteilung als Authentifizierungsmerkmal dienen um zu verhindern, dass Jugendliche nicht-jugendfreie Filme probeschauen. Auf die Tatsache, dass die Kundenkarten getaggt waren, wurden die Kunden – nach Aussage von RFID-Aktivisten – nicht hingewiesen.[262] Auch eine der bekanntesten RFID-Aktivistinnen – *Katherine Albrecht* – bekam eine solche Kundenkarte ausgehändigt. Ihr war ebenfalls nicht bewusst, dass die Karte getaggt war. Erst als sie die Karte zufällig bei einem Vortrag am nächsten Tag an ein RFID Lesegerät hielt, wurde klar, was wirklich „in der Karte steckte". Die Aktivisten beließen es allerdings nicht beim bloßen Auslesen der auf dem Tag gespeicherten Informationen. Sie demonstrierten vielmehr, dass auch das Verändern der Tag-Informationen mit dem entsprechenden technischen Equipment möglich ist, indem sie zusätzlich den Satz „Thank you, Katherine" auf dem Tag speicherten.[263] Nach Protestaktionen der Aktivisten entschloss sich METRO die getaggten Kundenkarten zurückzunehmen.[264]

Für die individuelle Identifizierung kommt aber auch die Kombination der zunächst anonym gesammelten Informationen über den betreffenden Kunden mit seinen Kreditkartendaten beim Bezahlen in Betracht. Eine zweite Möglichkeit ist die Anfertigung von Fotos in dem Moment, in dem ein Kunde ein Produkt aus dem Regal nimmt. Damit können Profile zu dem zwar namentlich unbekannten aber visuell bekannten Kunden erstellt werden. Ebenso lassen sich weitergehende Merkmale wie Geschlecht, Alter, gegebenenfalls sogar sozialer Status, des Betroffenen erkennen. Auch Bargeldzahler können damit erfasst werden. Diese Video"überwachung" in Kombination mit RFID als „Auslöser" mag dem ein oder andern fantastisch erscheinen. Faktisch ist dies – wenn auch nur im Rahmen eines Pilotprojektes – schon vorgekommen.[265]

e) Individual-Werbung

Namentlich identifizierten und profilierten Kunden kann ebenfalls sensitive Werbung[266] präsentiert werden. Durch die Kenntnis des Namens und entsprechend meist auch der Kontaktdaten kann der Verkäufer die Werbung allerdings nicht nur im Laden schalten, sondern dem Kunden beispielsweise auch per Post, E-Mail oder SMS zukommen lassen.

---

[262] Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, oben Fn. 110, S. 7. Anders stellt es ein Sprecher der METRO Group dar, nach dessen Aussage eine mündliche Aufklärung der Kunden über das RFID-Tag in der Karte stattgefunden habe, vgl. Auszug aus einem E-Mail Interview mit Daniel Kitscha, S. 7, 36 der STOA Studie.

[263] Heise News Meldung vom 02.02.2004, RFID beim Einkaufen: Danke, Katherine, abrufbar unter http://www.heise.de/newsticker/meldung/44237 (04.04.2013).

[264] Heise News Meldung vom 27.02.2004, Metro zieht RFID-Karte zurück, abrufbar unter http://www.heise.de/newsticker/meldung/45062 (04.04.2013).

[265] *Albrecht/McIntyre*, Spychips, S. 43 f., die berichten, dass 2003 Gillette und Tesco – eine britischen Kaufhauskette – eben dies versuchten.

[266] Vgl. hierzu *Flörkemeier/Schneider/Langheinrich*, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, oben Fn. 252, S. 6.

III. Leading Scenarios

Aus den oben genannten Anwendungsbereichen und herausgearbeiteten Szenarien lassen sich vier maßgebliche *Leading Scenarios*[267] bestimmen. Anhand dieser Szenarien wird im weiteren Verlauf der Arbeit die momentane Rechtslage darauf untersucht, ob sie ein hinreichendes Datenschutzniveau zum Schutz der Rechte des Einzelnen gewährleisten.

Aufgrund der unterschiedlichen denkbaren Ausgestaltungen der Anwendungsbereiche (es sind Daten auf dem Tag gespeichert oder aber in der Datenbank), kann es zu Überschneidungen bei der Einordnung zu den verschiedenen Szenarien kommen. Im Folgenden sollen nicht alle Anwendungsbereiche den Szenario-Typen zugeordnet werden, sondern lediglich die für diese Arbeit relevanten.

1. RTAMP

Bei der Zuordnung der RTAMP relevanten Anwendungsbereiche ist die Unterscheidung zwischen *intrinsic* und *extrinsic ubiquity*[268] zu berücksichtigen. Sowohl aus technischen als auch aus rechtlichen Gesichtspunkten unterscheiden sich beide Szenarien.

a) Intrinsic Ubiquity

Dem Bereich der *intrinsic ubiquity* unterfallen alle Anwendungsbereiche, bei denen Personen RFID-Chips implantiert werden. Hierzu gehört die Verwendung entsprechender Chips im Baja Beachclub, die Implantierung von Chips in Gefängnissen und anderen Einrichtungen sowie der aus medizinischen Gründen implantierte VeriChip. Bei implantierten Chips ist immer eine eindeutige Identifizierbarkeit des Trägers gegeben. Sei es, dass bereits direkt auf dem Chip Name und ähnliches gespeichert sind, oder aber lediglich eine dem EPC vergleichbare einzigartige Nummer enthalten ist und alle weiteren Daten in der Datenbank abgelegt sind.

b) Extrinsic Ubiquity

Extrinsic Ubiquity umfasst all die Anwendungsbereiche, bei denen der Betreffende lediglich dauerhaft einen getaggten Gegenstand bei sich führt und direkt auf dem Tag seine personenbezogenen Daten gespeichert sind. In diesen Fällen kann – soweit das Tag nicht verschlüsselt

[267] Die verwendeten Szenario-Bezeichnungen hat eingeführt *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 205; vgl. auch schon *Schmid*, Mastering the Legal Challenges *in*: Heinrich (Hrsg.), RFID and Beyond, S. 194; die Leading Scenarios werden in grau schraffierten Kästen dargestellt.

[268] Diese Differenzierung hat schon vorgenommen *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 205.

ist[269] – jeder die Daten auslesen. Sofern die Daten verschlüsselt sind, jedenfalls jeder, der den Schlüssel besitzt oder aber den Schutzmechanismus überwinden kann.[270]

Beim Pass und Personalausweis sind personenbezogene Daten direkt auf dem Tag gespeichert, insbesondere sogar Passfoto und teilweise auch die Fingerabdrücke des Betroffenen, vgl. § 4 Abs. 3 S. 1 PassG (Passbild und Fingerabdrücke) sowie § 5 Abs. 5 Nr. 1 und 3, Abs. 9 S. 1 PAuswG (Passbild immer, Fingerabdrücke nur auf Antrag des Betroffenen). Vergleichbares gilt für einige ÖPNV-Tickets.

2. AGG-EPC

Bei den denkbaren Aggregationsszenarien ist für diese Arbeit von Bedeutung die Variante AGG-EPC, also die Verknüpfung der Identifikationsnummer auf dem Tag mit personenbezogenen Daten des Betroffenen im Hintergrundsystem. Alle Fälle der Authentisierung, Authentifizierung und Autorisierung sind hier zu nennen. Sowohl beim elektronischen Schlüssel als auch bei bestimmten E-Tickets müssen die Daten der Kunden in einer Datenbank gespeichert sein. Gleiches gilt bei den Maut- und automatischen Bezahlsystemen. Auch hier sind die Kundendaten in einer Datenbank gespeichert, während der Kunde ein Tag am Auto oder Schlüsselbund trägt.

3. EPC

RFID-Einsatz auf Produktebene bedeutet zunächst, dass lediglich eine Produktidentifikationsnummer auf dem Tag gespeichert ist. Weder Name noch sonstige Daten der Kunden spielen eine Rolle. Entsprechend können dem EPC-Szenario grundsätzlich alle Anwendungsbereiche zugeordnet werden, bei denen Gegenstände getaggt und mit einer EPC-(oder sonstigen eindeutigen Identifikations-)Nummer versehen werden, ohne, dass die Daten der Kunden ebenfalls auf dem Tag gespeichert oder in der Datenbank mit den Produktdaten zusammengeführt werden. Die gesamten Anwendungen im Supermarkt, insbesondere Diebstahlsicherung, Lagerverwaltung, Inventur und Fälschungsschutz gehören hierzu. Auch der Bezahlvorgang fällt unter das reine EPC-Szenario, solange nicht die Kreditkartendaten mit den Produktdaten kombiniert und gespeichert werden, es also lediglich darum geht den Bezahlvorgang durch Ersetzung des Strichcodes zu beschleunigen. Wie oben dargestellt findet eine Verknüpfung mit Kundendaten bei den Maut-Systemen und auch im Baja Beachclub statt, sodass es hier gerade nicht bei einem EPC-Szenario bleibt. Nicht erfasst werden außerdem die Bereiche der Reklamation und Rückgabe, weil auch hier denknotwendigerweise eine Verknüpfung mit den Kundendaten geschehen muss.

---

[269] Vgl. zu den möglichen technischen Vorkehrungen zum Schutz von RFID-Tags gegen unbefugtes Auslesen der (Klar)Daten unten E.II.4. Zum Begriff der Verschlüsselung und den unterschiedlichen Verschlüsselungsmethoden vgl. *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 30 ff.

[270] Bei der Qualifizierung von Daten als personenbezogene kommt es maßgeblich darauf an, ob die sie erhebende Stelle die Daten im Klartext auslesen kann – dies ist der Fall, wenn die Daten unverschlüsselt sind oder die Stelle den Schlüssel innehat. Kann der Auslesende lediglich die verschlüsselte Version der Daten auslesen, erhält er nicht die dahinter stehenden personenbezogenen Daten sondern lediglich ein Substitut, den Chiffretext – es handelt sich für ihn also um andere Daten als für den Schlüsselinhaber, vgl. zu den Begriffen „Klartext“ und „Chiffretext“ *Gerhards*, (Grund-)Recht auf Verschlüsselung?, S. 30.

Wie oben gesehen können aber selbst mittels EPC individuelle Bewegungs- und sogar Kundenprofile erstellt werden. Dies ist einerseits möglich, ohne, dass der einzelne Kunde über ein bestimmtes Identifizierungsmerkmal identifiziert und damit wiedererkannt werden kann andererseits aber natürlich erst recht, wenn der Kunde zumindest über eine eindeutige Identifizierungsnummer bekannt ist.

4. Leading Scenarios – Kurzfassung

Zusammenfassen lassen sich die *Leading Scenarios* wie folgt:

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur weiterführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

D. Datenschutzrecht – Traditioneller Ansatz

Bei allen datenschutzrechtlich relevanten Szenarien stellt sich die Frage, ob der bestehende Rechtsrahmen ausreicht, um die statuierten Schutzziele zu erreichen, oder ob Anpassungen vorgenommen werden müssen. Für RFID-Anwendungen gilt nichts anderes. Im Folgenden soll daher der bestehende datenschutzrechtliche Rahmen auf europäischer und deutscher Ebene dargestellt und auf sein Schutzniveau in Bezug auf die oben herausgearbeiteten *Leading Scenarios* untersucht werden.

I. EU

EU-rechtliche Regelungen zum Datenschutz finden sich sowohl auf Primär- als auch auf Sekundärrechtsebene. Im Primärrecht, der Grundordnung der EU, verständigen sich die Mitgliedstaaten auf die elementaren Werte und Grundsätze, die im gemeinsamen Rechtsraum der EU gelten sollen. Das ursprüngliche Konvolut von Verträgen ist mittlerweile durch den Vertrag von Lissabon zusammengefasst worden. Eine der Konsequenzen des Vertrags von Lissabon ist die rechtlich verbindliche Anerkennung[271] der EU-Grundrechtecharta (GRCh). Deren Art. 8 statuiert nunmehr auch auf europäischer Ebene ein originäres Grundrecht auf Datenschutz. Gleichfalls wurde durch den Vertrag von Lissabon Art. 16 AEUV (ex-Art. 186 EU) eingefügt, der das Grundrecht auf den Schutz der personenbezogenen Daten nochmals betont und in Absatz 2 gleichfalls dem europäischen Gesetzgeber eine weitreichende Gesetzgebungskompetenz zur Regelung des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten einräumt.[272]

Zurzeit finden sich datenschutzrechtliche Regelungen auf Sekundärebene im Wesentlichen in zwei Richtlinien. Als erstes ist hier Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[273] (Datenschutzrichtlinie – DSRL) zu nennen. Ergänzt wird die Datenschutzrichtlinie durch Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[274] (Datenschutzrichtlinie für elektronische Kommunikation – eDSRL). Die Richtlinien binden die Mitgliedstaaten bei der Ausführung von EU-Recht. Sie bilden gleichzeitig die Grundlage für das nationale Datenschutzrecht der Mitglied-

---

[271] Vgl. Art. 1 Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13. Dezember 2007, ABl. C 306/1 vom 17. Dezember 2007, abrufbar unter http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:DE:HTML (04.04.2013).

[272] Die Kompetenz zum Erlass datenschutzrechtlicher Regelungen im Bereich der Gemeinsamen Außen- und Sicherheitspolitik ergibt sich aus Art. 39 S. 1 EU, vgl. auch *Bernsdorff* in: Meyer, Art. 8, Rn. 10a.

[273] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31 vom 23.11.1995, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML (04.04.2013).

[274] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201/37 vom 31.7.2002, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:de:HTML (04.04.2013).

staaten und wurden – wie von Art. 288 Abs. 3 EU (ex-Artikel 249 Abs. 3 EG) angeordnet – von diesen entsprechend umgesetzt. In Ergänzung der DSRL hat der Europäische Gesetzgeber 2001 eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr erlassen.[275] Diese Verordnung bindet aber, wie der Titel bereits zum Ausdruck bringt, lediglich die Gemeinschaftsorgane und -einrichtungen, nicht hingegen die Mitgliedstaaten. Zwar sind auch RFID-Szenarien denkbar, die unter den Anwendungsbereich der Verordnung fallen – z.B. an die Mitarbeiter eines Gemeinschaftsorgans ausgegebene RFID-Tokens als Türöffner – diese sollen hier aber unberücksichtigt bleiben. Im Übrigen ist der Regelungsgehalt der Verordnung mit der der DSRL vergleichbar, sodass auf die hierzu gemachten Ausführungen verwiesen wird.

Auch internationale Übereinkommen und Verträge können zur Regelung des Datenschutzes in den Mitgliedstaaten der EU Anwendung finden. Wegen ihres wesentlichen Einflusses auf das europäische Recht ist hier zunächst die Europäische Menschenrechtskonvention (EMRK)[276] des Europarates zu nennen. Ausgehend von Art. 8 Abs. 1 EMRK, der den Anspruch eines jeden Menschen auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Korrespondenz schützt, hat der Europarat 1980 das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten verabschiedet.[277] Das Datenschutzübereinkommen des Europarats stellt die ersten völkerrechtlich verbindlichen internationalen Datenschutzregeln dar. Nicht rechtlich bindend[278] sind demgegenüber die OECD Richtlinien zum Datenschutz und grenzüberschreitenden Datenverkehr[279] sowie die Richtlinien betreffend personenbezogene Daten in automatisierten Dateien der UNO[280].

Unabhängig von ihrer etwaigen Bindungswirkung für die EU-Mitgliedstaaten und die EU als solches, beschränkt sich diese Arbeit auf die Betrachtung des EU-Rechts als primäre Rechtsquelle bei der Bewertung datenschutzrechtlich relevanter Szenarien in der EU und ihren Mitgliedstaaten.

---

[275] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8/1 vom 12.1.2001, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:DE:PDF (04.04.2013).

[276] Europarat, Konvention zum Schutze der Menschenrechte und Grundfreiheiten (SEV Nr. 005), vom 4. November 1950, abrufbar unter http://www.echr.coe.int/NR/rdonlyres/F45A65CD-38BE-4FF7-8284-EE6C2BE36FB7/0/GER_CONV.pdf (04.04.2013).

[277] Europarat, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), vom 28. Januar 1980, abrufbar unter http://conventions.coe.int/treaty/ger/treaties/html/108.htm (04.04.2013).

[278] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 98 f.

[279] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Originalversion in Englisch), vom 23. September 1980, abrufbar unter http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html (04.04.2013).

[280] UNO Richtlinien betreffend personenbezogene Daten in automatisierten Dateien vom 14. Dezember 1990 (A/RES/45/95), abrufbar (englisch) unter http://www.un.org/documents/ga/res/45/a45r095.htm (04.04.2013).

1. Primärrecht: EU Grundrechtecharta

Seit dem am 1. Dezember 2009 in Kraft getretenen Vertrag von Lissabon[281] ist die Grundrechtecharta der EU Primärrecht und mit den Verträgen über die EU rechtlich gleichrangig.

> Artikel 6 EU
>
> (1) Die Union erkennt die Rechte, Freiheiten und Grundsätze an, die in der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind; die Charta der Grundrechte und die Verträge sind rechtlich gleichrangig.
>
> (…)

Die in ihr genannten Grundrechte gelten damit auch in den Mitgliedstaaten unmittelbar.[282] Gebunden werden durch sie allerdings nur die Gemeinschaftsorgane sowie die nationalen Organe der Mitgliedstaaten, soweit diese Gemeinschaftsrecht anwenden.

Zwar war die EU auch vor dieser Neuerung zur Achtung der Grundrechte verpflichtet (Achtung der Grundrechte der EMRK und der Mitgliedsstaaten, Art. 6 Abs. 2 EU a.F.), mit dem Vertrag von Lissabon und der Anerkennung der Grundrechtecharta hat der europäische Grundrechtsschutz allerdings eine neue Dimension erfahren.

Ausdrücklich normiert ist das Grundrecht auf Datenschutz in Art. 8 GRCh:

> Artikel 8 GRCh Schutz personenbezogener Daten
>
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Art. 8 GRCh stützt sich auf ex-Art. 286 EG sowie auf die DSRL und auf Art. 8 EMRK.[283] Auch wenn Art. 8 GRCh vom Schutz der personenbezogenen Daten spricht, ist doch vielmehr der Schutz des Einzelnen bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten gemeint.[284]

Weil Art. 8 GrCH stark an der DSRL orientiert ist und die entscheidenden Begriffe unverändert übernommen wurden, kann deren Inhalt und ihre Interpretation auch zur Auslegung von Art. 8 GrCH herangezogen werden.[285] Der Bezug zur DSRL darf indes nicht so verstanden werden, dass der Schutzbereich des Art. 8 GrCH lediglich einen ausgestaltungsbedürftigen Grundsatz bildet; vielmehr wird das Grundrecht zwar durch Sekundärrecht in seinem subjek-

---

[281] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13. Dezember 2007, ABl. C 306/1 vom 17. Dezember 2007, oben Fn. 271.

[282] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 110.

[283] *Bernsdorff* in: Meyer, Art. 8, Rn. 2; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 111.

[284] *Büllesbach*, RDV 2002, 55.

[285] Vgl. *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Kap. 7 § 5, Rn. 1361 ff.; *Johlen* in: Tettinger/Stern, Art. 8, Rn. 16; die starke Verschränkung mit dem sekundärrechtlichem EU-Datenschutzrecht macht in seiner Kommentierung auch deutlich *Bernsdorff* in: Meyer, Art. 8, Rn. 15, 16, 17, 18, 21, 22, 23.

tiven Gehalt konkretisiert und damit verstärkt – abgeschwächt werden kann sein Schutzbereich durch die Anlehnung an die DSRL hingegen freilich nicht.[286] Beschränkbar ist das Grundrecht auf Datenschutz über die besondere Schranke in Art. 52 Abs. 2 GRCh im Rahmen der Erlaubnistatbestände, die die DSRL statuiert.[287]

2. Sekundärrecht: Richtlinien 95/46/EG und 2002/58/EG

Die DSRL wurde im Oktober 1995 verabschiedet und – wenn auch größtenteils mit Verspätung[288] – in allen Mitgliedstaaten umgesetzt. Sie bildet die Basis des Datenschutzrechts in der EU und wird daher auch oft als allgemeine Datenschutzrichtlinie bezeichnet.[289] Die sie ergänzende eDSRL wurde im Juli 2002 verabschiedet. Sie ersetzt Richtlinie 97/77/EG[290] – die sog. „Telekom-Datenschutzrichtlinie".

a) Datenschutzrichtlinie 95/46/EG

Als Rahmen für den Datenschutz in der EU regelt die DSRL die Grundprinzipien, die bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten berücksichtigt werden müssen. Gestützt auf ex-Art. 100a EG normiert sie ein Niveau für den Datenschutz, das den ungehinderten Fluss personenbezogener Daten innerhalb der EU gewährleisten soll. Ziel ist die Herstellung eines gleichwertigen, hohen Datenschutzniveaus durch umfassende Harmonisierung.[291] Umfasst sind hierbei nicht lediglich grenzüberschreitende Sachverhalte, sondern auch die Durchdringung der einzelstaatlichen Regelungen und damit ihre Integration.[292] Der EuGH hat hierzu im Fall *Bodil Lindqvist*[293] klargestellt:

- Die Harmonisierung der nationalen Rechtsvorschriften ist nicht auf eine Mindestharmonisierung beschränkt, sondern führt zu einer grundsätzlich umfassenden Harmonisierung. Die DSRL will den freien Verkehr personenbezogener Daten sicherstellen, wobei sie zugleich ein hohes Niveau des Schutzes der Rechte und Interessen der von diesen Daten betroffenen Personen gewährleistet.[294]

---

[286] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Kap. 7 § 5, Rn. 1364.

[287] *Bernsdorff* in: Meyer, Art. 8, Rn.17, der allerdings darauf hinweist, dass die (umstrittene) Anwendung der besonderen Grundrechtsschranke des Art. 52 Abs. 2 GRCh eine Folge der Einführung von Art. 16 AEUV ist.

[288] Schweden war das einzige Land, das die Umsetzungsfrist wahrte. Mit der Umsetzung 2001 verpasste Deutschland das Umsetzungsziel um drei Jahre.

[289] *Kuner*, European Data Protection Law, S. 19.

[290] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. L 24/1 vom 30.01.1998, abrufbar unter http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=DE&numdoc=31997L0066&model=guichett (04.04.2013).

[291] Erwägungsgründe 8 und 10 der DSRL, oben Fn. 273.

[292] *Brühann* in: Grabitz/Hilf (Hrsg.), RL 95/46/EG Vorbemerkung: Datenschutz und die Europäische Gemeinschaft, Rn. 43, f.

[293] EuGH Urteil vom 6.11.2003 – Rs. C-101/01 – Bodil Lindqvist, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62001J0101:de:HTML (04.04.2013).

[294] EuGH Urteil vom 6.11.2003 – Rs. C-101/01 – Bodil Lindqvist, oben Fn. 293, Rn. 95, 96.

- Die Mitgliedstaaten sind nicht gehindert, die Geltung der Richtlinie auf Bereiche auszudehnen, die von ihrem Anwendungsbereich an sich nicht erfasst werden.[295]
- Die Mitgliedstaaten müssen allerdings bei der Schaffung nationaler Regelungen ausdrücklich ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre wahren.[296]

In einem Spannungsverhältnis stehen nach diesen Vorgaben des EuGH einerseits das Ziel einer umfassenden Harmonisierung des Datenschutzrechts in der EU und andererseits die Aufforderung an die Mitgliedstaaten ein möglichst hohes Niveau für den Datenschutz zu schaffen. Der Bezug der DSRL zum Funktionieren des Binnenmarktes (ex-Art. 100a Abs. 1 EG) kann dahingehend interpretiert werden, sie sowohl als Unter- als auch als Obergrenze für nationalstaatliche Datenschutzregeln zu verstehen.[297] Dies macht auch Sinn, gilt es doch zum Zwecke der Gewährleistung eines reibungslosen Datenverkehrs innerhalb der EU zu verhindern, dass die Mitgliedstaaten in einen – politisch oder wirtschaftlich motivierten – Wettlauf um den höchsten oder niedrigsten Datenschutz eintreten.[298]

aa) Anwendungsvoraussetzungen

Gemäß Art. 1 DSRL unterfällt dem Anwendungsbereich der DSRL grundsätzlich jede Verarbeitung personenbezogener Daten. Art. 3 Abs. 1 DSRL konkretisiert dies dahingehend, dass die DSRL „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen“, gilt. Lediglich die in Art. 3 Abs. 2 DSRL genannten Ausnahmen führen zu einer Nichtanwendbarkeit der DSRL auf die dort benannten Datenverarbeitungsprozesse: Einerseits betrifft dies die Verarbeitung personenbezogener Daten im Zusammenhang mit der Wahrung der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und Tätigkeiten des Staates im strafrechtlichen Bereich sowie Tätigkeiten der Mitgliedstaaten außerhalb des Anwendungsbereiches des Gemeinschaftsrechts; andererseits Datenverarbeitungen einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Der Europäische Gesetzgeber hat damit zum Ausdruck gebracht, dass es – so wie es auch das Bundesverfassungsgericht sieht[299] – grundsätzlich kein belangloses Datum mehr gibt.

Im konkreten Fall ist mithin zu prüfen, ob *personenbezogene Daten* vorliegen, diese i.S.d. DSRL *verarbeitet* werden und, ob *keine Ausnahme* vom Anwendungsbereich gegeben ist.

---

[295] EuGH Urteil vom 6.11.2003 – Rs. C-101/01 – Bodil Lindqvist, oben Fn. 293, Rn. 98, 99.

[296] EuGH Urteil vom 6.11.2003 – Rs. C-101/01 – Bodil Lindqvist, oben Fn. 293, Rn. 97, 99.

[297] So die Ansicht der Kommission in EuGH Urteil vom 6.11.2003 – Rs. C-101/01 – Bodil Lindqvist, oben Fn. 293, Rn. 94.

[298] Zum Spannungsverhältnis *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 122 f.

[299] BVerfGE 65, 1 (45) – Volkszählung.

Weiterhin gilt es zu klären, wer Adressat der Regeln der DSRL ist; dies ist gem. Art. 6 Abs. 2 DSRL der *für die Datenverarbeitung Verantwortliche*.

aaa) Personenbezogene Daten

Der Begriff der personenbezogenen Daten ist Dreh- und Angelpunkt jedes datenschutzrechtlichen Szenarios. Weil Datenschutzrecht darauf abzielt, den Einzelnen bei der Verarbeitung personenbezogener Daten vor Verletzungen seines Persönlichkeitsrechts zu schützen, müssen personenbezogene Daten betroffen sein, um überhaupt die Anwendbarkeit von Datenschutzrecht legitimieren zu können.

Nach der Definition in Art. 2 a) DSRL sind

> a) "personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

So wesentlich die Qualifizierung betroffener Daten als personenbezogene ist, so schwer fällt in vielen Fällen die Subsumtion des konkreten Sachverhalts unter die o.g. Definitionsmerkmale. Mit zunehmender Technisierung und den sich hieraus ergebenden Möglichkeiten der Überwachung und Profilbildung müssen zunehmend auch auf den ersten Blick „harmlose“ – weil nicht offensichtlich mit der betroffenen Person verknüpfte oder auf sie hinweisende – Daten auf ihre Qualität als personenbezogene untersucht werden. Den sich hieraus ergebenden Klärungsbedarf hat die Artikel-29-Datenschutzgruppe erkannt und sich der Auslegungsfragen in einer eigens hierzu ergangenen Stellungnahme angenommen.[300] Gleich zu Beginn der Stellungnahme hebt die Datenschutzgruppe hervor, dass die Auslegung des Begriffs der personenbezogenen Daten unter anderem in RFID-Anwendungen von besonderer Bedeutung ist.[301]

Die Einschätzungen der Artikel-29-Datenschutzgruppe sind zwar nicht unmittelbar bindend für die Mitgliedstaaten und die Auslegung nationalen Rechts. Allerdings teilt die Gruppe ihre Arbeitsergebnisse, Erkenntnisse und Einschätzungen der Kommission mit und berät diese (insbes. Art. 30 Abs. 1 c), Abs. 2 DSRL). Sie soll vornehmlich zu einer einheitlichen Anwendung der DSRL beitragen (Art. 30 Abs. 1 a) DSRL). Ihr kommt damit ein indirekter aber nicht zu unterschätzender Einfluss auf die datenschutzrechtliche Gesetzgebung und die Auslegung bestehenden Datenschutzrechts in der EU zu, der die Mitgliedstaaten zumindest dazu anhält, sich an den Vorgaben der Gruppe zu orientieren.

Aus der Definition des Begriffs personenbezogener Daten ergibt sich eine logische Unterteilung in vier Begriffsmerkmale, die die Datenschutzgruppe einzeln analysiert. Personenbezogene Daten sind

---

[300] Artikel-29-Datenschutzgruppe, WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20.06.2007, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf (04.04.2013).

[301] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 3.

- „alle Informationen“ (*Informationen*)
- „über“ (*Bezug*)
- „eine bestimmte oder bestimmbare“ (*Bestimmbarkeit*)
- „natürliche Person“ (*Betroffener*).

i. Informationen

Mit der Formulierung *alle* Informationen hat der Europäische Gesetzgeber klar zum Ausdruck gebracht, dass der Begriff der personenbezogenen Daten denkbar weit zu fassen ist. Die Qualifizierung soll nicht bereits am Begriff Informationen scheitern; die Eingrenzung soll vielmehr erst später – beim Merkmal der Bestimmbarkeit – erfolgen. Folglich fallen zunächst alle Arten von Aussagen über eine Person unter den Begriff Informationen: objektive (also Fakten, die den Betroffenen beschreiben), subjektive (alle Meinungen und Werturteile des und über den Betroffenen), wahre und unwahre (auch ein Gerücht kann untrennbar mit einer Person verknüpft sein), sensible und allgemeine, aus dem Privat- und Familien- oder Berufsleben.[302] In welcher Form die Aussage vorliegt – schriftlich, elektronisch, akustisch, grafisch etc. – ist unerheblich.[303] Auch biometrische Daten (Fingerabdrücke, Iris-Scans, aber auch Bewegungs- oder sonstige Verhaltensmuster) erfüllen den Begriff der Information.[304] Dies ist in Bezug auf RFID beachtlich, wenn man bedenkt, dass in den neuen Ausweispapieren neben den klassischen Identifikationsmerkmalen – Name, Geburtsort und -tag etc. – nunmehr auch solche Daten gespeichert werden und mittels RFID-Chip auslesbar sind (s.o.B.II.5.a)).

Nicht als Information ist hingegen das Material zu qualifizieren, aus dem die entsprechende Information ermittelt werden kann: die Blutprobe, aus der sich die Blutgruppe des Betroffenen ermitteln lässt, unterfällt nicht dem Begriff der Information, die ermittelte Blutgruppe hingegen schon.[305]

ii. Bezug

Das Merkmal „über“ beschreibt die Komponente des Personen*bezugs*. Ob Informationen einen solchen Bezug zu einer natürlichen Person aufweisen, ist in vielen Fällen nicht eindeutig.

Unproblematisch ist der Bezug zu bejahen, wenn Informationen ohne weiteren Zwischenschritt, also insbesondere ohne weitergehende Ermittlungen, *einer* Person zugeordnet werden können (z.B. namentlich geführte Akten, Bildaufnahmen etc.).[306]

Schwieriger sind Konstellationen, in denen die gegebenen Informationen unmittelbar mit einem Gegenstand verknüpft sind. Sofern der betreffende Gegenstand einer Person gehört, einem Einfluss durch oder auf die Person unterliegt oder irgendeine Art von physischer oder

[302] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 7.

[303] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 8.

[304] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 9.

[305] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 10.

[306] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 10.

räumlicher Nähe zu einer Person aufweist, kann hierüber gegebenenfalls ein indirekter Bezug zur Person hergestellt werden.[307]

Diese Situation stellt sich auch in vielen RFID-Anwendungen, in denen natürliche Personen mit getagten Gegenständen umgeben sind und solche bei sich haben. Entsprechend weist die Artikel-29-Datenschutzgruppe auch darauf hin, dass das Bezugselement eine wichtige Rolle bei der Beurteilung der inhaltlichen Dimension des Begriffs der personenbezogenen Daten, insbesondere im Zusammenhang mit Gegenständen und neuen Technologien, spielt.[308]

In ihrem Arbeitspapier zu Datenschutzfragen der RFID-Technik[309] äußert sich die Artikel-29-Datenschutzgruppe wie folgt:

> „Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird."[310]

Hieraus hat die Datenschutzgruppe eine Unterteilung in drei Subkategorien abgeleitet.[311] Informationen können demzufolge einen Personenbezug aufweisen, wenn sie ein *Inhaltselement*, ein *Zweckelement* oder ein *Ergebniselement* aufweisen. Diese drei Elemente müssen hierbei nicht kumulativ sondern können alternativ vorliegen, um den Personenbezug zu bewirken.[312]

Das *Inhaltselement* beschreibt die Datenschutzgruppe dabei wie folgt:

> „Das „Inhaltselement" ist immer dann vorhanden, wenn – nach dem allgemein üblichen Verständnis des Wortes „beziehen" – Informationen über eine bestimmte Person gegeben werden, und zwar unabhängig vom Zweck aufseiten des für die Verarbeitung Verantwortlichen oder eines Dritten oder von den Auswirkungen dieser Information auf die betroffene Person. Informationen „beziehen" sich auf eine Person, wenn es sich um Informationen „über" diese Person handelt, und dieser Punkt ist unter Berücksichtigung aller Begleitumstände zu beurteilen."[313]

Der hier herangezogene Zirkelschluss macht deutlich, wie schwierig die Annäherung an das Bezugsmerkmal ist. Für den Bezug („über" wie in der Begriffsdefinition der personenbezogenen Daten verwendet) ein Inhaltselement genügen zu lassen, welches gegeben sein soll, wenn es sich um Informationen „über" die Person handelt, hilft bei der Rechtsanwendung schließlich nicht weiter. Nichts desto trotz schlägt die Datenschutzgruppe hier den Bogen zurück zu RFID-basierten Ausweispapieren und belegt die auf dem RFID-Tag des Personalausweises oder Reisepasses gespeicherten Daten mit der Qualifizierung des Inhaltselements.[314]

---

[307] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 10.

[308] Artikel-29-Datenschutzgruppe, WP 136, S. 29.

[309] Artikel-29-Datenschutzgruppe, WP 105, Arbeitspapier Datenschutzfragen im Zusammenhang mit der RFID-Technik, 19.01.2005, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf (04.04.2013).

[310] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 9.

[311] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 11.

[312] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 13.

[313] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 11.

[314] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 11.

Was sich hier so – scheinbar – intuitiv ergibt, ist mit Worten schwer zu fassen. Löst man sich von der unglücklichen Formulierung, die die Artikel-29-Datenschutzgruppe gewählt hat, kann man das Inhaltselement bejahen, wenn Informationen vorliegen, die unmittelbare Rückschlüsse auf eine Person zulassen, auch wenn die betreffende Person noch nicht identifiziert – i.S.v. individualisierbar – ist. Als Beispiel kann die DNA eines Straftäters herangezogen werden, die am Tatort gefunden wird: Zwar ist der Täter noch nicht – namentlich – bekannt, es ist aber klar, dass die DNA *einer* Person[315] – nämlich dem Täter – zugewiesen werden kann.

Das *Zweckelement* soll gegeben sein,

> „wenn die Daten unter Berücksichtigung aller Begleitumstände mit dem Zweck verwendet werden bzw. verwendet werden könnten, eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen."[316]

Nach der Beschreibung des *Ergebniselements* sollen Daten auch deshalb als personenbezogen qualifiziert werden können,

> „weil sich ihre Verwendung unter Berücksichtigung aller jeweiligen Begleitumstände auf die Rechte und Interessen einer bestimmten Person auswirken könnte."[317]

Die Datenschutzgruppe weist ausdrücklich darauf hin, dass das Alternativverhältnis der Elemente dazu führt, dass das gleiche Datum auf verschiedene Personen beziehbar sein kann, wenn etwa Informationen „über" Person 1 dazu verwendet werden, um Person 2 auf eine bestimmte Art und Weise zu behandeln (z.B. der Sohn wird 25 Jahre alt, deshalb erhält der verbeamtete Vater fortan keinen Ortszuschlag mehr).[318]

iii. Bestimmbarkeit

Mit dem Merkmal der Bestimmbarkeit setzt sich die Artikel-29-Datenschutzgruppe am intensivsten auseinander. Dies ist nicht verwunderlich, steht und fällt mit ihm doch die Qualifizierung von Daten als personenbezogene i.S.d. Definition in der DSRL. Es ist insofern darauf hinzuweisen, dass auch Daten, die zunächst einen Bezug wie unter ii. dargestellt aufweisen – und damit wörtlich genommen personen*bezogene* sind – nicht zwangsläufig unter den Begriff der personenbezogenen Daten i.S.d. DSRL fallen. Dies rührt daher, dass eine Gefährdung des Persönlichkeitsrechts da ausgeschlossen ist, wo der Betroffene anonym bleibt.

> Erwägungsgrund 26 DSRL
>
> (…) Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. (…)

Anonym ist eine Person zunächst dann, wenn ihre Identität von niemandem ermittelt werden kann. Eine solche Person ist weder bestimmt noch bestimmbar i.S.d. Definition der personenbezogenen Daten. Im Umkehrschluss ist eine Person bestimmt, wenn ihre Identität feststeht, sie sich also in einer Personengruppe von allen anderen Mitgliedern der Gruppe unterschei-

---

[315] Und selbst hier ergeben sich Unsicherheiten, bilden doch eineiige Mehrlinge die Ausnahme.

[316] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 11 f.

[317] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 13.

[318] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 14.

det.[319] Dies ist der Fall, wenn bei Betrachten der gegebenen Informationen klar ist, wer gemeint ist.[320] Das ist unproblematisch dann der Fall, wenn das gewählte Merkmal in der Gruppe nur einmal vorkommt (die einzige Frau in einer Gruppe Männer). Treffen auf mehrere Personen einer Gruppe gleiche Identifikationsmerkmale zu, so müssen weitere Merkmale hinzutreten, um eine eindeutige Unterscheidung zu ermöglichen (nicht Petra Müller sondern Petra Meier). In diesem Fall ergibt sich die Bestimmtheit erst über die Kombination mehrerer Merkmale (z.B. Vorname und Nachname).[321] Die Artikel-29-Datenschutzgruppe macht hier besonders deutlich, dass die Herstellung des Bezugs nicht gleichbedeutend ist mit der namentlichen Identifizierung[322], sprich die Kenntnis der „sozialen Identität“[323] des Betroffenen.

Bestimmbar ist eine Person laut Definition in Art. 2 a) DSRL, wenn sie *direkt* oder *indirekt* identifizierbar ist. Die Identifikation kann nach der Definition erfolgen durch Mittel wie insbesondere der Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck der physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der Person ist. Die Datenschutzgruppe wendet die Begriffe direkt und indirekt erstaunlicherweise sowohl auf die Bestimmtheit als auch die Bestimmbarkeit an.[324] Dem eindeutigen Wortlaut der Definition in der DSRL zu Folge soll dies aber nur bei der Bestimmbarkeit gelten. Dies macht auch Sinn, schließlich ist eine bestimmte Person immer direkt bestimmt; eine Auswahlmöglichkeit besteht nicht und es besteht auch kein Bedarf an weitergehenden Informationen. Dies gilt sowohl, wenn lediglich ein bekanntes Merkmal herangezogen werden muss, um den Betroffenen zweifelsfrei zu identifizieren, als auch, wenn dies erst durch die Kombination mehrerer bekannter Merkmale möglich ist.[325]

Bei bloßer Bestimmbarkeit ist die zweifelsfreie Identifikation des Betroffenen mit den bekannten Merkmalen gerade nicht möglich. Es bedarf in diesen Fällen also immer einer Kombination mit weiteren – zunächst unbekannten – Merkmalen. Hierbei ergeben sich zwei Fallgruppen, die in ihrer weiteren Betrachtung unterschiedlich bewertet werden können.

Einerseits ist denkbar, dass der datenverarbeitenden Stelle bereits ein Merkmal bekannt ist, das aber zur Identifikation noch nicht ausreicht, weitere die Identifikation ermöglichende Informationen aber ebenfalls bei ihr *vorhanden* sind. Dies ist beispielsweise denkbar, bei Konzernen, die Kunden- oder Beschäftigtendaten in verschiedenen Datenbanken speichern. Auf der anderen Seite kann es aber auch sein, dass sich die weiteren für die Identifikation erforderlichen Informationen bei einer anderen datenverarbeitenden Stelle befinden.

---

[319] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 14.

[320] *Saeltzer*, DuD 2004, 218.

[321] *Saeltzer*, DuD 2004, 218.

[322] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 16.

[323] Artikel-29-Datenschutzgruppe, WP 175, Stellungnahme 5/2010 zum Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen, vom 13.07.2010, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_de.pdf (04.04.2013), S. 9.

[324] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 15 f.

[325] Diesbezüglich zutreffend Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 15.

Diese Unterscheidung ist wichtig, weil der Gesetzgeber nicht alle Identifikationsmöglichkeiten von der DSRL umfasst sehen wollte:

> Erwägungsgrund 26 DSRL
>
> (…) Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. (…)

Die Vorgabe des Gesetzgebers ist, dass nicht jede rein hypothetische Möglichkeit der eindeutigen Identifikation dazu führt, dass der Betroffene als bestimmbar i.S.d. DSRL anzusehen ist. Insoweit bleibt zu klären, inwieweit die Heranziehung von Mitteln – mit dem Wortlaut, den der Europäische Gesetzgeber gewählt hat – noch als *vernünftig* einzustufen ist und ab wann lediglich eine hypothetische Möglichkeit besteht, den Betroffenen tatsächlich eindeutig zu identifizieren.

Nach Einschätzung der Artikel-29-Datenschutzgruppe sind hierbei verschiedene Faktoren zu berücksichtigen. Die Kosten sind dabei ein wichtiger, aber nicht der einzige Faktor. Auch der Zweck, die Strukturierung der Verarbeitung, der von dem für die Datenverarbeitung Verantwortlichen erwartete Vorteil, die auf Seiten des Betroffenen zu erwartende Eingriffsintensität sowie die Gefahr organisatorischer und technischer Fehler sollen zu berücksichtigen sein.[326] Gleichzeitig weist die Datenschutzgruppe auf die Dynamik technischer Entwicklungen hin. Bei der Frage der Beziehbarkeit sollte der Stand der Technik berücksichtigt werden, der zu dem Zeitpunkt vorherrscht, in dem die Daten *verarbeitet* werden.[327] D.h., dass es maßgeblich auf die Lebens- also Speicherdauer der betreffenden Daten ankommt und eine Prognoseentscheidung vorzunehmen ist. Erhebungs- und Verarbeitungszeitpunkt können auseinanderfallen – und tun dies regemäßig auch. Während es für Daten, die lediglich kurze Zeit gespeichert werden – z.B. IP-Adressen bei Internetzugangsanbietern[328] – auch nur der momentane Stand der Technik zu berücksichtigen sein soll, ist für Daten, die über Jahre, gar Jahrzehnte gespeichert und zu einem oder mehreren Zeitpunkten der Speicherdauer verarbeitet werden sollen, eine Prognose im Hinblick auf die technischen Möglichkeiten für den entsprechenden Zeitpunkt anzustellen. Der Hintergrund für diese Forderung ist, dass zum jetzigen Zeitpunkt nicht absehbar ist, ob Daten, die heute „belanglos“ erscheinen, in der Zukunft nicht mit einfachsten Mitteln – und von einem dementsprechend großen Personenkreis – dem Einzelnen zugeordnet werden können (vgl. nur die Entwicklungen auf dem Gebiet der Gesichtserkennungssoftware, die von jedermann mit Bilderdatenbanken kombiniert werden kann[329]).

---

[326] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 18.

[327] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 18.

[328] Dies gilt jedenfalls so lange, wie der Gesetzgeber die Vorgaben des BVerfG zur Vorratsdatenspeicherung nicht gesetzlich umgesetzt und die Vorratsdatenspeicherung wieder gesetzlich verpflichtend ist; BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, abrufbar unter http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (04.04.2013) = BVerfGE 125, 260 – Vorratsdatenspeicherung.

[329] Heise Online News vom 29.06.2011, Datenschützer warnen vor flächendeckender Gesichtserkennung, abrufbar unter http://www.heise.de/newsticker/meldung/Datenschuetzer-warnen-vor-flaechendeckender-Gesichtserkennung-1269926.html (04.04.2013).

Im oben erwähnten Konzern-Beispiel erscheint die Kombination der erforderlichen Informationen bereits zum jetzigen Zeitpunkt nicht übermäßig aufwändig. Im Einzelfall kommt es selbstverständlich auf die vorhanden Unternehmensstrukturen und Datenverarbeitungssysteme an, jedoch kann hier eine Kombination der Daten mit vernünftigerweise heranzuziehenden Mitteln unterstellt werden. Anders sieht dies indes im o.g. zweiten Beispiel aus: Auf die bei einer anderen Stelle gespeicherten Informationen kann die datenverarbeitende Stelle nicht ohne weiteres zugreifen. Hier wird es zum jetzigen Zeitpunkt im Einzelfall auf die Mitwirkungsbereitschaft der anderen Stelle ankommen, die zudem (datenschutz-)rechtlichen Einschränkungen unterliegt. Denkbar ist aber, dass künftige Technologien diesen Zugriff – wenn auch möglicherweise nicht rechtmäßig so aber doch faktisch – ermöglichen. Eine abschließende Prognose kann hier schwer gestellt werden. Im Ergebnis heißt dies, dass sofern die Erlangung der fehlenden Daten mit vernünftigerweise heranzuziehenden Mitteln möglich ist, die bei *beiden* Stellen gespeicherten Daten – auch wenn jeweils für sich genommen nicht ausreichend für eine eindeutige Identifizierung des Betroffenen – als personenbezogene Daten zu qualifizieren sind.

Dies stellt datenverarbeitende Stellen vor eine große Herausforderung: Verzichten sie, um eventuellen datenschutzrechtlichen Verpflichtungen in der Zukunft aus dem Weg zu gehen, von vornherein auf die Verarbeitung solcher Daten, deren Einstufung in der Zukunft nicht absehbar ist, oder führen sie solche Verarbeitungen durch und wenn ja, unter welchen Bedingungen. In letzterem Falle wird sich regelmäßig anbieten, die Voraussetzungen für eine datenschutzrechtlich verträgliche Verarbeitung jedenfalls soweit wie möglich vorzubereiten, um später relevanten gesetzlichen Verpflichtungen so einfach wie möglich nachkommen zu können.

iv. Betroffener

Die DSRL beschränkt ihren Anwendungsbereich auf natürliche Personen (vgl. Art. 1 Abs. 1 DSRL).[330] Daten „über" juristische Personen sind ausgeschlossen, nicht aber Daten natürlicher Personen, die bei einer juristischen Person vorhanden sind (Beschäftigten-, Kundendaten). Zu berücksichtigen ist indes, dass sich Informationen nach der Bezugsdefinition der Artikel-29-Datenschutzgruppe gleichzeitig auf mehrere Personen beziehen können. Entsprechend ist im Einzelfall zu klären, ob Informationen „über" eine juristische Person gleichzeitig – durch Heranziehung des Zweck- oder Ergebniselements – auch einen Bezug zu einer natürlichen Person aufweisen.[331]

Die DSRL verbietet es den Mitgliedstaaten indes nicht, in den Anwendungsbereich ihrer Datenschutzgesetze auch Daten juristischer Personen mit einzubeziehen. Von dieser Möglichkeit

[330] *Brühann* in: Grabitz/Hilf (Hrsg.), RL 95/46/EG Art. 1. Gegenstand der Richtlinie, Rn. 6.

[331] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 27; vgl. für die Regelung im BDSG VG Wiesbaden, NVwZ-RR 2008, 617: „Wirtschaftsdaten einer juristischen Person sind personenbezogene Daten einer natürlichen Person, wenn diese einer Person als Alleinaktionär oder Gesellschafter zuzurechnen sind."

haben einige Mitgliedstaaten Gebrauch gemacht.[332] Der deutsche Gesetzgeber hat hingegen Daten über juristische Personen nicht dem Anwendungsbereich des BDSG unterstellt.[333]

v. Personenbeziehbare Daten – Eine neue Kategorie?

Im Zusammenhang mit massenhafter Datenerhebung und -verarbeitung in der informatisierten Welt ist der Ausdruck „personen*beziehbare* Daten“ aufgekommen. Dieser zeichne sich dadurch aus, dass die in Frage stehenden Daten (noch) nicht eindeutig einer Person zuzuordnen seien. Die prinzipielle Möglichkeit der Herstellung eines solchen *Bezugs* zwischen der betroffenen Person und den Daten bestünde indes und werde insbesondere womöglich in der Zukunft bestehen; erst unter Hinzuziehung weiterer Daten könne die zugeordnete Person ermittelt werden.[334] Die Begriffswahl verwirrt indes. Nach obigen Ausführungen ist Folgendes zu berücksichtigen: Daten *beziehen* sich immer auf eine oder mehrere Personen. Alle menschgemachten bzw. von Menschen besessenen Gegenstände weisen einen oder mehrere Bezüge zu einer oder mehreren Personen auf. Folgendes Beispiel mag dies verdeutlichen: Ein getaggter Gegenstand wird von einem Lesegerät zu einem Zeitpunkt X an einem Ort Y erfasst. Da der Gegenstand nicht selbstständig dorthin gelangt ist, steht fest, dass eine Person Z ihn dorthin verbracht hat. Das RFID-Tag des Gegenstands weist damit Person Z Zeitangabe X sowie Ortsangabe Y zu. Wer Person Z (namentlich) ist, mag für die verantwortliche Stelle (noch) nicht erkennbar sein. Dass diesen Bezug nicht jedermann herstellen kann, ändert aber nichts an der Bejahung des *Bezugselements* i.S.d. Definition des Begriffs der personenbezogenen Daten. Relevanz gewinnt dieser Faktor hingegen bei der Qualifizierung von Tag-Nummer, Orts- und Zeitangabe als personenbezogene Daten insgesamt. Die Unsicherheiten im Hinblick auf dieses Fehlen des „Bezugs“ adressiert der europäische Gesetzgebers indes bereits in der DSRL und zwar – wie oben ausgeführt – im Rahmen des *Bestimmtheitselements*, vgl. Erwägungsgrund 26.

Der Einführung eines neuen Begriffs der „personen*beziehbaren* Daten“ bedarf es von daher *de lege lata* nicht. Aus Verständnisgründen kann er zur Verdeutlichung des Umfangs des Begriffs der personenbezogenen Daten eben auch auf *potenziell* personenbezogene Daten Sinn machen. Dann muss aber deutlich sein, dass er sich nicht nur auf das Bezugselement der Definition sondern auf die Definition insgesamt bezieht.

---

[332] Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 28.

[333] Vgl. *Gola/Schomerus*, BDSG, § 3 Rn. 11.

[334] Vgl. zuletzt den Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, abrufbar unter http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20111212/Ausschussdrucksache_17_24_42.pdf (04.04.2013), S. 27; *Saeltzer*, DuD 2003, 218 (219); Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 109; vgl. auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, abrufbar unter http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile (04.04.2013), S. 61.

vi. Leading Scenarios

Im Folgenden sollen die oben herausgearbeiteten *Leading Scenarios* und die dort betroffenen Daten auf ihre Qualität als personenbezogene Daten i.S.d. Definition der DSRL untersucht werden.

Szenario 1:

(1) RTAMP – Extrinsic Ubiquity[335]:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

Auf dem RFID-Tag selbst gespeicherte Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck o.ä. sind regelmäßig und insbesondere in Kombination als personenbezogene Daten zu qualifizieren. Das Bezugselement ist unproblematisch gegeben. Nach den Ausführungen der Artikel-29-Datenschutzgruppe ist in diesen Fällen bereits das Inhaltselement zu bejahen, schließlich handelt es sich um Informationen „über" den Betroffenen, die also ohne weiteren Zwischenschritt *einer* Person zugeordnet werden können. Ob der Betroffene dann als Konsequenz in einer bestimmten Hinsicht behandelt werden soll (Zweckelement) oder ob sich die Verwendung der Daten in sonstiger Weise auf seine Rechte und Interessen auswirken könnte (Ergebniselement), spielt also keine Rolle mehr. Gleichfalls ist der Betroffene für die datenverarbeitende Stelle auch regelmäßig bestimmt, also eindeutig identifizierbar. Der Hintergrund für die Speicherung entsprechender Daten verfolgt nämlich gerade den Zweck, den Inhaber des Ausweispapiers oder sonstigen Gegenstandes zweifelsfrei identifizieren zu können, weswegen gerade bei Ausweispapieren wie dem Pass oder dem Personalausweis nicht lediglich ein sondern mehrere Merkmale gespeichert werden, die eine Verwechslung ausschließen. Dies betrifft auch dritte datenverarbeitende Stellen, also andere als die Tag-ausgebende Stelle, sofern auf die gespeicherten Daten Zugriff besteht und sich über die Kombination der Merkmale eine eindeutige Identifikationsmöglichkeit des Betroffenen ergibt.

In Szenario 1 finden die datenschutzrechtlichen Vorschriften der DSRL und folglich auch der nationalen Datenschutzgesetze damit vollumfänglich Anwendung und die Verarbeitung der Daten ist an deren Rechtmäßigkeitsvoraussetzungen zu messen.

Szenario 2:

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

In Szenario 2 muss zwischen zwei Datenkategorien unterschieden werden: Einerseits der Identifikationsnummer auf dem RFID-Tag und andererseits den im Hintergrundsystem gespeicherten Daten.

[335] Vgl. zu den Begrifflichkeiten schon oben Fn. 267.

Die (RFID-Tag-)Identifikationsnummer ist als Kennnummer i.S.d. Definition in Art. 2 a) DSRL und damit als personenbezogenes Datum zu qualifizieren. Zwar ist die Nummer zunächst dem RFID-Tag zugeordnet. Mit der Implantierung verliert dieses aber seine Eigenständigkeit und es wird eine unmittelbare und untrennbare Verbindung mit dem Betroffenen hergestellt. Damit wird die Nummer – die zunächst nur eine Information „über" das RFID-Tag war – zu einer Information „über" den Betroffenen: Die Nummer ist mit genau *einer* Person verbunden, nicht mit mehreren. Gleichzeitig ist diese Person auch eindeutig identifizierbar. Für die eindeutige Identifizierbarkeit ist nämlich, wie oben festgestellt, keine namentliche oder an sonstigen konventionellen persönlichen Merkmalen festzumachende Zuordnung erforderlich.[336] Für die datenverarbeitende Stelle ist bei Erfassen der Identifikationsnummer klar, dass die Nummer genau *einer* Person, nämlich dem Betroffenen, zugeordnet ist. Bezugs- und Bestimmtheitselement fallen hier also zwangsläufig zusammen.

Die sonstigen im Hintergrundsystem gespeicherten Daten sind zudem ebenfalls personenbezogene Daten für die datenverarbeitende Stelle, entsprechen sie doch in ihrer Qualität den in Szenario 1 betrachteten Daten. Dies betrifft aber nur die Stelle, die tatsächlich Zugriff auf die Daten hat, nicht auf externe dritte Stellen, die zwar die RFID-Tag-Nummer erheben und dadurch ggf. Bewegungs- und Kundenprofile anlegen können aber keinen Zugriff auf das Hintergrundsystem haben.

Auch in Szenario 2 finden die datenschutzrechtlichen Vorschriften damit uneingeschränkt Anwendung und zwar sowohl für die Stelle, die die Implantierung des RFID-Tags veranlasst und damit auf eine Vielzahl von Daten Zugriff hat – für diese Stelle also hinsichtlich beider Datenkategorien – als auch für dritte datenverarbeitende Stellen, die lediglich die auf dem RFID-Tag gespeicherte Identifikationsnummer auslesen – für solche Stellen nur bezüglich dieser Identifikationsnummer.

Szenario 3:

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

Szenario 3 unterscheidet sich von Szenario 2 dadurch, dass das ausgegebene RFID-Tag, auf dem eine Identifikationsnummer gespeichert ist, nicht in den Körper des Betroffenen implantiert, es aber regelmäßig vom Betroffenen mitgeführt wird. Im Hintergrundsystem sind wiederum weitergehende Daten über den Betroffenen gespeichert. Auch hier ist zwischen den verschiedenen Datenkategorien zu unterscheiden, nämlich einerseits der RFID-Tag-Nummer und andererseits den im Hintergrundsystem gespeicherten Daten.

Die im Hintergrundsystem gespeicherten Daten sind ebenso wie in Szenario 2 für die Tag ausgebende Stelle, die Zugriff auf die Daten hat, als personenbezogene Daten zu qualifizieren. Insoweit ergibt sich kein Unterschied.

[336] Vgl. hierzu speziell für RFID-Anwendungen Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S.9.

Differenzierter ist indes die Qualifizierung der auf dem RFID-Tag gespeicherten Identifikationsnummer. Die Bejahung des Bezugselements bereitet hierbei zunächst Schwierigkeiten.

Für den eindeutigen Personenbezug fehlt es in diesem Szenario an der dauerhaften Verbindung mit einer Person. Fraglich ist, ob die Nummer dennoch eine Kennnummer i.S.d. Definition der personenbezogenen Daten ist. Kennnummern zeichnen sich dadurch aus, dass sie *einer* Person zugeordnet werden, um diese zweifelsfrei identifizieren zu können. Grundsätzlich ließe sich dies auch bei Kundenkarten u.ä. bejahen, will doch die ausgebende Stelle die Verknüpfung zwischen Karteninhaber, Karte bzw. RFID-Tag-Nummer und den Daten im Hintergrundsystem und damit dem bestimmungsgemäßen Karteninhaber eindeutig herstellen können. Dies gilt insbesondere, wenn die Karte eine Bezahlfunktion hat. Allerdings steht es im faktischen Belieben des Betroffenen, die Karte Dritten auszuhändigen, unabhängig von der Frage, ob diese die Karte im Einzelhandel oder ihrer sonstigen Bestimmung nach benutzen oder nicht. Bei Erfassen der RFID-Tag-Nummer durch die kartenausgebende oder eine dritte datenverarbeitende Stelle während des Beisichführens der Karte durch einen Dritten würde folglich nicht das Bewegungsprofil des Karteninhabers sondern eben das des Dritten erstellt. Eine die RFID-Tag-Nummer auslesende Stelle kann damit nie sicher sein, dass der Träger der Karte auch deren bestimmungsgemäßer Inhaber und damit immer *dieselbe* Person ist. In der Realität werden Kundenkarten zwar wahrscheinlich regelmäßig nicht vom Karteninhaber an Dritte herausgegeben. Die bloße Möglichkeit hingegen genügt zur Verneinung des von der Artikel-29-Datenschutzgruppe herausgearbeiteten Inhaltselements, weil die Identifikationsnummer *im Zweifel* eben kein Datum „über“ *eine* Person ist.

Infolge der Gegenstandsbezogenheit der RFID-Identifikationsnummer gibt es in diesem Szenario also zwei potenzielle Betroffenengruppen: Zum einen der bestimmungsgemäße Inhaber des getaggten Gegenstandes und zum anderen Dritte, denen der bestimmungsgemäße Inhaber den Gegenstand aushändigt. Die von der Artikel-29-Datenschutzgruppe herausgearbeiteten Kriterien zur Bejahung des Bezugselements stoßen hier an ihre Grenzen. Eine mögliche Konsequenz wäre, sämtlichen gegenstandsbezogenen RFID-Identifikationsnummern die Qualität als personenbezogene Daten abzusprechen. Fraglich ist, ob dies sachgerecht ist. Das von einer ubiquitären RFID-Umgebung ausgehende latente Gefahrenpotenzial für das Persönlichkeitsrecht des Einzelnen – eben auch des Dritten – besteht nämlich weiterhin.

Das Bezugselement ist nach den Ausführungen der Artikel-29-Datenschutzgruppe weiterhin bei Vorliegen des Zweck- oder Ergebniselements zu bejahen. Hierbei gilt, dass auch eine fremde Kundenkarte bzw. die auf ihr gespeicherte Nummer dazu verwendet werden kann, ihren Träger in einer bestimmten Hinsicht zu behandeln. So ist denkbar, dass auch ein Dritter beim Einkauf bei dem kartenausgebenden Unternehmen einen Rabatt erhält, weil mit der Karte in der Vergangenheit ein hoher Umsatz getätigt wurde. Umgekehrt ist vorstellbar, dass die Abgabe bestimmter Produkte an den die Karte Vorlegenden verweigert wird, etwa, weil der berechtigte Karteninhaber in dem betreffenden Geschäft Hausverbot erhalten hat. Das wären Beispielsfälle für das Vorliegen des Zweckelements. Das noch weitere Ergebniselement könnte in allen Situationen bejaht werden, in der das Beisichführen der getaggten Karte eine

irgendwie geartete Auswirkung auf den Träger haben *könnte*[337]. Eine schier unbegrenzte Ausweitung des Bezugselements ist die Folge.

Ausdrücklich für RFID-Anwendungen betont die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme zum ersten Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen eine sehr restriktive Zweifelseinschätzung:

> „Somit ist es also selbst in den Fällen, in denen ein RFID-Tag lediglich eine in einem bestimmten Kontext eindeutige Nummer und keine weiteren personenbezogenen Daten enthält, geboten, mögliche Datenschutz- und Sicherheitsaspekte sorgfältig zu erwägen, wenn der RFID-Tag von Personen mitgeführt werden soll. (…)Wie bereits in Abschnitt 2.2 hervorgehoben, **enthält ein RFID-Tag, der von einer Person** (einem Nutzer oder einer Einzelperson) **mitgeführt wird und eine eindeutige Kennung enthält, per definitionem personenbezogene Daten** [Hervorhebungen eingef. d. Verf.].“[338]

In der Stellungnahme zum überarbeiteten zweiten Vorschlag der Branche wiederholt sie diese Einschätzung.[339]

Es muss indes hinterfragt werden, ob man in solchen Fällen wirklich noch von einem Bezug i.S.d. zweiten Merkmals der Definition sprechen kann, oder, ob die Einschätzungen der Artikel-29-Datenschutzgruppe hier nicht über das Ziel hinausgehen. Ohne stichhaltige Begründung davon auszugehen, dass Identifikationsnummern auf produktbezogenen RFID-Tags keinen Personenbezug aufweisen[340], ist sicherlich ebenso als vorschnell anzusehen, wie einen solchen ohne Betrachtung der Gefahrenlage und der praktischen Konsequenzen anzunehmen. Teilweise werden Daten wie in diesem Szenario beschrieben als solche „ohne gezielten Personenbezug“ qualifiziert und für sie ein neues Regelungsregime gefordert.[341]

Das Ziel der Artikel-29-Datenschutzgruppe ist zweifelsohne die Gewährleistung eines möglichst umfassenden Schutzes des Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts. Nichts desto trotz gilt es auch den Grundsatz der Normenklarheit zu beachten. Eine klare Begründung, warum Identifikationsnummern getaggter Gegenstände, die von Einzelpersonen mitgeführt werden, als personenbezogene Daten i.S.d. DSRL zu qualifizieren sind, bleibt die Artikel-29-Datenschutzgruppe schuldig. Insofern soll im Folgenden eine Begründungsmöglichkeit aufgezeigt werden.

Unter Heranziehung eines weiteren (ungeschriebenen) Merkmals im Rahmen der Auslegung der Definition der personenbezogenen Daten käme man zu einer sachgerechten Lösung. Die-

---

[337] Die Artikel-29-Datenschutzgruppe verwendet hier in der Tat den Begriff „könnte“, Artikel-29-Datenschutzgruppe, WP 136, oben Fn. 300, S. 13.

[338] Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 9, 11.

[339] Artikel-29-Datenschutzgruppe, WP 180, Stellungnahme 9/2011 zu dem überarbeiteten Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen, vom 11.02.2011, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_de.pdf (04.04.2013), S. 5; zum gleichen Ergebnis kommt auch Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 208: „...sind Kennnummern der RFID-Tags in oder an den Objekten in Hinblick auf ihren Träger praktisch immer personenbeziehbare Daten.“

[340] So sehen es *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 92 f.; *v. Westerhold/Döring*, CR 2004, 710 (714); *Holznagel/Bonnekoh*, MMR 2006, 17 (21); *Huber*, MMR, 2006, 728 (733).

[341] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 68.

ses Merkmal ist das der *Zeit*. In einem bestimmten Zeitraum ist nämlich die Identifikationsnummer einer weitergegebenen Kundenkarte ein Datum „über" den jeweiligen Träger und keine andere Person. Der Bezug geht folglich verloren, sobald der getaggte Gegenstand den Besitzer wechselt. Dann ist die auf dem RFID-Tag gespeicherte Nummer wiederum eine Information „über" den neuen Träger.

Sieht man diese Herangehensweise noch im Rahmen zulässiger Auslegung, so stellen sich weitere Schwierigkeiten beim dritten Merkmal der Definition, nämlich der Bestimmtheit bzw. der Bestimmbarkeit des Betroffenen, die parallel zu den Problemen hinsichtlich des Bezugselements verlaufen: In dem Zeitraum, in dem die RFID-Tag-Nummer *einer* Person zugeordnet werden kann (Bezugselement) ist diese Person auch zweifelsfrei zu identifizieren: Nur sie ist Träger des betreffenden RFID-Tags. Über die Person können dann Profile angelegt und sie verfolgt werden. Allerdings geht auch die Möglichkeit der Identifizierung *dieser* von Anderen unterscheidbaren Person verloren, sobald der Gegenstand weitergegeben wird. Dann kann wiederum nur der neue Träger zweifelsfrei identifiziert werden. Auch hier spielt demnach die zeitliche Komponente die ausschlaggebende Rolle. Etwas anderes gilt nur, wenn im entsprechenden Zeitraum weitere Identifikationsmerkmale durch die datenverarbeitende Stelle erhoben werden, wie beispielsweise die Verknüpfung von Bildaufnahmen einer Überwachungskamera mit der RFID-Tag-Nummer.

In der Konsequenz reduziert sich das Gefährdungspotenzial für das Persönlichkeitsrecht des Betroffenen zwar, es besteht aber in gewissem Umfang fort: Faktisch kann eine datenverarbeitende Stelle ohne Erhebung weiterer Identifikationsmerkmale eine bestimmte Person nur verfolgen und Profile von ihr anlegen, solange mit Sicherheit davon ausgegangen werden kann, dass der mit dem RFID-Tag versehene Gegenstand nicht an einen Dritten weitergegeben wurde. In der Praxis würde das in Bezug auf eine Kundenkarte bedeuten, dass bei jedem Einkauf ein neues, von anderen unabhängiges Profil angelegt würde. Bewegungs- und Verhaltensprofile können damit zwar immer noch angelegt werden, aber eben nur noch solche über einen *kurzen Zeitraum* und in einer eng umgrenzten überschaubaren Umgebung.

Im Ergebnis ist damit der Artikel-29-Datenschutzgruppe in ihrer Einschätzung zuzustimmen, dass auch Identifikationsnummern auf mit RFID getaggten Gegenständen als personenbezogene Daten zu qualifizieren sind. Das Gefährdungspotenzial für das geschützte Rechtsgut – das Persönlichkeitsrecht des Betroffenen – ist indes ein anderes, im Vergleich zu Daten i.S.v. Szenario 2, bei denen die Identifikationsnummer durch Implantierung zu personenbezogenen Daten werden, oder aber den „sozialen" Identifikatoren, egal ob wie in Szenario 1 direkt auf dem Tag oder wie in Szenario 2 und 3 im Hintergrundsystem gespeichert, reduziertes.

Szenario 4:

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur weiterführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

Szenario 4 unterscheidet sich auf den ersten Blick nur unwesentlich von Szenario 3. Zwar entfällt die Beurteilung von im Hintergrundsystem gespeicherter Daten. Aber die auf dem RFID-Tag gespeicherten Daten entsprechen denen in Szenario 3 – lediglich eine gegenstands- bzw. in diesem Fall produktbezogene – eindeutige Identifikationsnummer ist gespeichert. Dennoch weist das Szenario bezüglich des Gefährdungspotenzials eine wiederum andere Qualität auf als Szenario 3. Zu berücksichtigen ist nämlich, dass es sich bei den getaggten Gegenständen in Szenario 4 regelmäßig um Verbrauchsgegenstände handelt. Das heißt, sie werden vom Betroffenen im Supermarkt ergriffen, bezahlt, nach Hause gebracht und irgendwann die Verpackung samt RFID-Tag entsorgt. Die Ausnahme bilden hier Kleidungsstücke und Accessoires, die der Betroffene ggf. auch über einen längeren Zeitraum immer wieder bei sich hat und die im Laufe ihrer Lebensdauer – z.B. als Secondhand-Ware – auch den Besitzer wechseln können. Die Möglichkeit konsistente Bewegungs- und Verhaltensprofile anzulegen oder den Betroffenen zu verfolgen reduziert sich damit noch einmal im Vergleich zu Szenario 3, welches wie festgestellt bereits eine andere Qualität als Szenarien 2 und 1 aufweist.

Szenario 4 weist im Vergleich sicherlich das geringste Gefährdungspotenzial für den Einzelnen auf. Indes darf nicht unberücksichtigt bleiben, dass es gleichzeitig das Szenario mit den meisten Anwendungsfällen sein wird, sofern RFID flächendeckend auf Produktebene zum Einsatz kommen sollte – wofür alle Zeichen sprechen. Das heißt, dass der Einzelne zwar im Hinblick auf jedes einzelne RFID-Tag wahrscheinlich keine schwerwiegenden Persönlichkeitsrechtsverletzungen zu fürchten hat, er aber auf der anderen Seite immer und überall mit einer RFID-Infrastruktur umgeben ist. In dieser Welt des *ubiquitous computing*[342] wird es immer schwieriger zu überblicken, welche RFID-Tags man gerade bei sich hat, wo diese gegeben falls ausgelesen werden und wie diese Daten dann im weiteren Verlauf von wem verwendet werden. Dies gilt insbesondere vor dem Hintergrund, dass mit zunehmendem technischem Fortschritt die Preise für die einzelnen Systemkomponenten immer weiter fallen und die erforderliche Hardware damit einem immer größer werden Personenkreis zugänglich sein werden. In Zukunft könnten Lesegeräte für den privaten Gebrauch von Jedermann eingesetzt werden – und das auch für illegitime Zwecke. Unterstützt wird dies durch von der Wirtschaft vorangetriebene Standardisierungsbestrebungen.

Die Tatsache, dass nach obiger Einschätzung, die auch die Artikel-29-Datenschutzgruppe teilt, auch die auf simplen produktbezogenen RFID-Tags gespeicherten Identifikationsnummern, sofern sie von Personen mitgeführt werden, personenbezogene Daten sind, stellt die Wirtschaft vor enorme Herausforderungen. Mit der Qualifizierung als personenbezogene Da-

[342] Vgl. bereits oben unter C.I.1.

ten ist der Anwendungsbereich des Datenschutzrechts und damit der Pflichtenkatalog für die datenverarbeitenden Stellen in der DSRL und den nationalen Datenschutzgesetzen eröffnet.[343]

vii. Zwischenergebnis

Maßgebliches Merkmal zur Unterscheidung der verschiedenen Gefährdungspotenziale ist, ob die verantwortliche Stelle, also nicht zwingend die Stelle, die das Tag ausgibt, sondern diejenige, die es im konkreten Fall ausliest, Zugriff auf nach konventionellem Verständnis personenbezogene Daten hat. Eine solche Zugriffsmöglichkeit setzt zunächst voraus, dass überhaupt irgendwo solche Daten gespeichert sind, sei es auf dem Tag selbst – wie in *Leading Scenario* 1 – oder aber in einem Hintergrundsystem – so wie in *Leading Scenarios* 2 und 3. *Leading Scenario* 2 nimmt insoweit eine Sonderstellung ein, als – wie ausgeführt – hier die Identifikationsnummer des Tags durch die Implantierung desselben für sich bereits zum konventionellen personenbezogenen Datum i.S. einer Kennnummer wird. Insoweit kommt es hierbei jedenfalls solange nicht auf die im Hintergrundsystem gespeicherten Daten an, wie die Identifikationsnummer unverschlüsselt übertragen wird, sodass sie grundsätzlich jedermann auslesen kann.

In den *Leading Scenarios* 1, 2 und 3 besteht damit grundsätzlich immer jedenfalls potenziell die Möglichkeit für die auslesende Stelle neben der Identifikationsnummer auch auf konventionelle Identifikatoren Zugriff zu erhalten. Für die Tag ausgebende Stelle gilt dies immer. Für dritte Stellen kommt es auf die konkreten Umstände an. Maßgeblich ist, *wie wahrscheinlich* es im Rahmen einer Prognoseentscheidung (vgl. beim Bestimmtheitselement, iii.) ist, dass ein solcher Zugriff *in der Zukunft* möglich sein wird. Ausgeschlossen dürfte dies nie sein. Eine Grenze ist mit dem europäischen Gesetzgeber aber dort zu ziehen, wo lediglich eine hypothetische Möglichkeit verbleibt, die Zugriffsmöglichkeit also nahezu ausgeschlossen ist.

Lediglich in *Leading Scenario* 4 gibt es die Möglichkeit des Zugriffs auf konventionelle Identifikatoren nicht, weil solche nirgends gespeichert sind. (Die Möglichkeit nachträglich eine solche Verknüpfung beispielsweise mit den Daten einer Kundenkarte herzustellen, ist nicht spezifisch für RFID. Hat eine nachträgliche Verknüpfung stattgefunden, liegt ein Fall von *Leading Scenario* 3 vor.)

Aber selbst da, wo für die Tag auslesende und damit für die Datenverarbeitung verantwortliche Stelle keine Zugriffsmöglichkeit auf konventionelle personenbezogene Daten besteht, ergibt sich vor dem Hintergrund der Möglichkeit der Auslesbarkeit der Identifikationsnummer ein Datenschutzrisiko. Dieses führt im Ergebnis dazu, dass nach momentaner Rechtslage und obiger Auslegung auch solche Daten als personenbezogene zu qualifizieren sind.

[343] Einen Personenbezug bei produktbezogenen Identifikationsnummern lehnt ab Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 208 f., weil es an einem „direkten Personenbezug“ fehle. Stattdessen geht man dort davon aus, dass zunächst nur „personenbeziehbare“ Profile erstellt werden können. Weil solche Daten aber im Kontext mit anderen (personenbezogenen) Daten auf eine Person schließen lassen könnten, werden sie im Ergebnis dennoch als unter die Definition der personenbezogenen Daten subsumiert, weil es sich insofern um Daten einer *bestimmbaren* Person handele.

bbb) Verarbeitung

Sofern im konkreten Fall personenbezogene Daten vorliegen, müssen diese i.S.d. DSRL verarbeitet werden. Nach der Definition in Art. 2 b) DSRL ist die

> b) "Verarbeitung personenbezogener Daten" ("Verarbeitung") jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

Der Verarbeitungsbegriff in der DSRL geht damit über den im BDSG gewählten (vgl. unten D.II.2.b)aa)) hinaus. Bereits das Erheben der Daten, also ihre erstmalige Erlangung, ist umfasst, sodass die Anwendbarkeit der DSRL selten an diesem Merkmal scheitern wird. Sämtliche Verarbeitungsformen haben sich an den Rechtmäßigkeitsvoraussetzungen gemäß Kapitel II der DSRL zu orientieren.

ccc) Keine Ausnahme vom Anwendungsbereich

Datenverarbeitungsmaßnahmen, die einen der Tatbestände aus Art. 3 Abs. 2 DSRL erfüllen, sind vom Anwendungsbereich ausgeschlossen. Im Einzelnen sind dies solche

- die für die Ausübung von Tätigkeiten erfolgen, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen,
- betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich, sowie
- die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden.

ddd) Für die Verarbeitung Verantwortlicher

Der für die Datenverarbeitung Verantwortliche ist als Normadressat eine zentrale Figur in jedem datenschutzrechtlichen Szenario: Ihn treffen die meisten Pflichten und Verantwortlichkeiten aus Kapitel II der DSRL ebenso wie etwaige Haftungspflichten und Sanktionen bei Zuwiderhandlungen, Art. 23 und 24 DSRL.[344]

Gemäß Art. 2 d) DSRL ist

> d) "für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden.

[344] *Kuner*, Christopher, European Data Protection Law, S. 70.

Sofern eine natürliche Person alleine oder mit anderen zusammen – etwa in einer Personengemeinschaft – über die Zwecke und Mittel der Verarbeitung entscheidet, ist diese problemlos als der für die Datenverarbeitung Verantwortliche zu erkennen. Gehört die Datenverarbeitung zum Geschäftsbetrieb einer juristischen Person, ist Verantwortlicher die juristische Person und wegen der Vertretungswirkung *nicht* die natürliche Person – Geschäftsführer, Vorstand, sonstiger Mitarbeiter – die die Datenverarbeitung tatsächlich steuert.[345]

In Abgrenzung zu den für die Datenverarbeitung Verantwortlichen sind Auftragsverarbeiter zu bringen. Nach der Definition in Art. 2 e) DSRL ist

> e) "Auftragsverarbeiter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

In unübersichtlichen Konzernstrukturen ist besonderes Augenmerk auf die Unterscheidung zu legen, die vielfach nicht eindeutig sein wird.[346] Hinzukommend ist denkbar, dass mehrere Personen als für die Datenverarbeitung Verantwortliche zu qualifizieren sind; dann treffen auch all diese Personen die Pflichten aus der DSRL. Globalisierung, zunehmende Vernetzung, dezentrale Datenspeicher- und -verarbeitungseinrichtungen führen zudem dazu, dass die Grenzen zwischen Verantwortlichem und Auftragsverarbeiter zunehmend verschwimmen: Daten werden gemeinsam – im Verbund – verarbeitet aber Verantwortlichkeiten aufgeteilt. Aus Unternehmersicht ist es aus Compliance-Gründen äußerst wichtig, zu klären, ob das Konzernunternehmen Verantwortlicher oder aber lediglich Auftragsverarbeiter ist.

bb) Anwendbares nationales Recht

Art. 4 DSRL regelt die territoriale Geltung der DSRL und das Recht welchen Mitgliedstaates für einen konkreten Datenverarbeitungsprozess anwendbar ist. Nach Art. 4 Abs. 1 a) und b) DSRL ist auf die betreffende Niederlassung des für die Datenverarbeitung Verantwortlichen abzustellen. Sofern ein für die Datenverarbeitung Verantwortlicher eine Niederlassung im Hoheitsgebiet eines Mitgliedsstaates bzw. an einem Ort, an dem das Recht dieses Mitgliedstaates Anwendung findet (insb. diplomatische und konsularische Vertretungen[347]), unterhält, gilt das Recht dieses Mitgliedstaates. Zudem ist im Falle mehrerer Niederlassungen in mehreren Mitgliedstaaten das Recht aller betroffenen Mitgliedstaaten, jeweils für die entsprechende Niederlassung, anzuwenden. Es kommt damit nicht auf die Person des Betroffenen, die Belegenheit der verwendeten Datenverarbeitungsanlagen oder die Lokalisierung der betreffenden Daten an.[348] Eine Niederlassung ist nach Erwägungsgrund 19 der DSRL auch gegeben bei Agenturen und Zweigstellen. Gleichfalls kommt es auf die Rechtsform der Niederlassung nicht an. Mit dieser Regelung soll verhindert werden, dass auf ein und dieselbe Datenverarbeitung das Recht gleich mehrerer Mitgliedstaaten angewendet werden muss.[349] Diese Regelung führt außerdem dazu, dass die nationalen Datenschutzbehörden, die jeweils die Einhal-

[345] *Damman/Simitis*, EG-Datenschutzrichtlinie, Art. 2 Rn. 11.

[346] *Kuner*, Christopher, European Data Protection Law, S. 70 f.

[347] *Damman/Simitis*, EG-Datenschutzrichtlinie, Art. 4 Rn. 5.

[348] *Brühann* in: Roßnagel, HdB DSR, 2.4 Europarechtliche Grundlagen, Rn. 23.

[349] *Brühann* in: Roßnagel, HdB DSR, 2.4 Europarechtliche Grundlagen, Rn. 25.

tung der Datenschutzgesetze überwachen, auch das Recht anderer Mitgliedstaaten anwenden müssen.[350]

Nach Art. 4 Abs. 1 c) DSRL kommt mitgliedstaatliches Recht auch dann zur Anwendung, wenn eine Niederlassung im betreffenden Mitgliedstaat zwar nicht vorhanden ist, wohl aber im Mitgliedstaat belegene Datenverarbeitungsanlagen vom für die Datenverarbeitung Verantwortlichen benutzt werden, sofern die Anlagen nicht lediglich für die Durchfuhr durch EU-Territorium verwendet werden. Damit soll verhindert werden, dass im Gebiet der EU datenverarbeitende Stellen durch Auslagerung ihres Sitzes in einen Drittstaat ihrer Verantwortlichkeit nach europäischem Datenschutzrecht entziehen. Sofern Verantwortliche daher zum Zwecke der Datenverarbeitung auf im Gebiet der EU belegene „Mittel zurückgreifen", diese also beherrschen, sind sie dem Regelungsregime der DSRL zu unterwerfen.[351]

Die Regelung des Art. 4 Abs. 1 c) DSRL wird zunehmend an Bedeutung gewinnen. Immer mehr Daten werden dezentral gespeichert und verarbeitet (u.a. mittels *Cloud Computing*[352]), ohne, dass der für die Datenverarbeitung Verantwortliche zwangsläufig auch einen Sitz im Land der Datenverarbeitung hat. Die für das „Internet der Dinge" und andere RFID-Infrastrukturen anzulegenden Datenbanken und Hintergrundsysteme werden auf der ganzen Welt – und damit in der „Cloud" – verstreut sein.

cc) Rechtmäßigkeitsvoraussetzungen für die Datenverarbeitung

In Kapitel II der DSRL finden sich die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Pflichtiger ist der für die Datenverarbeitung Verantwortliche. Der Auftragsverarbeiter ist gem. Art. 17 Abs. 3 zweiter Spiegelstrich DSRL mit verantwortlich für die Einhaltung der Vorgaben in Art. 17 Abs. 1 DSRL, nämlich die Gewährleistung der Sicherheit personenbezogener Daten bei der Verarbeitung.

Die genaue Ausgestaltung der Voraussetzungen obliegt gem. Art. 5 DSRL den Mitgliedstaaten. Daher wird im Folgenden lediglich kurz dargestellt, welche Rahmenbedingungen der europäische Gesetzgeber vorgesehen hat. Das Kapitel zum deutschen Recht wird sich vertieft mit einzelnen Rechtmäßigkeitsvoraussetzungen auseinandersetzen.

Es ist darauf hinzuweisen, dass der europäische Gesetzgeber nach nunmehr über 15 Jahren Gültigkeit der DSRL eine umfassende Überarbeitung der selbigen plant.[353] Im Januar 2012 hat die zuständige Kommissarin *Reding* Entwürfe für eine neue Datenschutzgrundverordnung[354] sowie für eine neue Datenschutzrichtlinie[355] vorgestellt. Während die Datenschutz-

---

[350] *Weichert* in: Däubler/Klebe/Wedde/Weichert, § 1 Rn. 16.

[351] *Damman/Simitis*, EG-Datenschutzrichtlinie, Art. 4 Rn. 6.

[352] Vgl. einführend Leupold/Glossner/*Stögmüller*, Münchener Anwaltshandbuch IT-Recht, Teil 5 Rn. 330 ff.; zu den datenschutzrechtlichen Herausforderungen beim Cloud Computing *Heidrich/Wegener*, MMR 2010, 803 ff.

[353] Die DSRL wurde erst einmal und nur unwesentlich geändert – mit Wirkung zum 20.11.2003 wurde Artikel 31 ersetzt.

[354] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung),

grundverordnung den Datenschutz in der EU einheitlich regeln soll, soll die neue Richtlinie künftig nur noch die Datenverarbeitung durch Polizei und Justiz neu regeln.[356] Bis zum 15. Januar 2011 hatten Interessierte die Möglichkeit ihre Stellungnahmen zu der entsprechenden Mitteilung der Kommission[357] im Rahmen einer öffentlichen Konsultation der Kommission abzugeben.[358] Die von der Kommission in ihrer Mitteilung angesprochenen Änderungspotenziale werden ebenfalls kurz dargestellt, könnten sie doch in Zukunft zu entsprechenden Änderungen in den mitgliedstaatlichen Datenschutzgesetzen führen.

In Art. 5 DSRL sind zunächst die Grundsätze von Treu und Glauben, der Zweckbindung – sowohl in sachlicher als auch in zeitlicher Hinsicht –, der Verhältnismäßigkeit sowie der Richtigkeit geregelt. Diese Grundsätze werden in den Folgevorschriften konkretisiert.[359] So sind Datenverarbeitungen lediglich dann legitim, wenn einer der in Art. 7 DSRL genannten Erlaubnistatbestände gegeben ist. Dies ist dann der Fall, wenn der Betroffene eingewilligt hat, Art. 7 a) DSRL, oder die Verarbeitung für einen der in Art. 7 b) bis f) DSRL genannten Fälle – u.a. Vertragserfüllung sowie Erfüllung einer rechtlichen Verpflichtung – erforderlich ist. Auch die Verarbeitung zur Verwirklichung des berechtigten Interesses des für die Datenverarbeitung Verantwortlichen kann als legitime Begründung für die Datenverarbeitung herangezogen werden, Art. 7 f) DSRL, allerdings muss dann eine Abwägung mit den schutzwürdigen Interessen und Grundrechten des Betroffenen stattfinden.

Art. 8 DSRL stellt – aufgrund der besonderen Gefährdungslage für das Persönlichkeitsrecht – besonders hohe Anforderungen an die Verarbeitung besonderer Kategorien personenbezogener Daten – Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit des Betroffenen hervorgehen, sowie Daten über Gesundheit oder Sexualleben. Die Verarbeitung solcher Daten ist gem. Art. 8 Abs. 1 DSRL grundsätzlich verboten und nur ausnahmsweise, bei Vorliegen der besonders strengen Voraussetzungen in den Absätzen 2 bis 7, zulässig.

KOM(2012) 11 endgültig vom 25.01.2012, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF (04.04.2013).

[355] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr KOM(2012) 10 endgültig 25.01.2012, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:PDF (04.04.2013).

[356] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Der Schutz der Privatsphäre in einer vernetzten Welt - Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endgültig vom 25.1.2012, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:DE:PDF (04.04.2013), S. 4.

[357] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endgültig, 04.11.2010, abrufbar unter http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf (04.04.2013).

[358] Europäische Kommission, Consultation on the Commission's comprehensive approach on personal data protection in the European Union, abrufbar unter http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm (04.04.2013).

[359] Vgl. *Kuner*, European Data Protection Law, S. 20.

Ein weiterer, wichtiger Grundsatz in der DSRL ist der der Transparenz. Entsprechend werden dem für die Datenverarbeitung Verantwortlichen umfassende Informationspflichten gegenüber dem Betroffenen auferlegt, Art. 10 und 11 DSRL, und der Betroffene bekommt Auskunftsrechte sowie Berichtigungs-, Löschungs- und Sperrungsansprüche gegenüber dem für die Datenverarbeitung Verantwortlichen eingeräumt, Art. 12 DSRL. Die Beschränkbarkeit der o.g. Rechte und Pflichten ist den Mitgliedstaaten nur in dem geringen in Art. 13 DSRL vorgegebenen Rahmen erlaubt.

Gem. Art. 17 DSRL haben – wie oben bereits angesprochen – sowohl der für die Datenverarbeitung Verantwortliche als auch der Datenverarbeiter dafür Sorge zu tragen, dass die Datenverarbeitung sicher ist. Sie müssen hierfür die geeigneten technischen und organisatorischen Maßnahmen durchführen, die für den Schutz der Daten gegen die zufällige oder unrechtmäßige Einflussnahme und Verarbeitung erforderlich sind.

In Art. 18 bis 21 DSRL finden sich Vorschriften zur Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen. So geht die DSRL grundsätzlich von einer Meldepflicht des für die Datenverarbeitung Verantwortlichen gegenüber einer national zu errichtenden Kontrollstelle vor Aufnahme der Datenverarbeitungstätigkeit aus, Art. 18 Abs. 1 DSRL. Die Kontrollstelle hat ihre Tätigkeit in völliger Unabhängigkeit auszuüben, Art. 28 Abs. 1 DSRL. Dieses Kriterium erfüllen die mit der Kontrolle der Datenverarbeitung des nicht-öffentlichen Bereichs beauftragten Stellen der Bundesländer in Deutschland zum jetzigen Zeitpunkt nicht, weil sie staatlicher Aufsicht unterworfen sind. Entsprechendes hat der EuGH im Rahmen einer von der Kommission erhobenen Vertragsverletzungsklage nach ex-Art. 226 EG festgestellt.[360] Die Landesgesetzgeber sind infolgedessen zum Handeln verpflichtet, um die entsprechenden deutschen Regelungen und Strukturen europarechtskonform anzupassen. In Art. 18 Abs. 2 DSRL werden die Ausnahmen von der Meldepflicht aufgelistet. Die wohl wichtigste und vom deutschen Gesetzgeber im BDSG aufgegriffene Ausnahme ist die Bestellung eines unabhängigen Datenschutzbeauftragten (betrieblicher Datenschutzbeauftragter) durch den für die Datenverarbeitung Verantwortlichen, der die Einhaltung der datenschutzrechtlichen Vorgaben überwacht.

Kapitel III der DSRL adressiert die Rechtsbehelfe des Betroffenen bei Verletzung der datenschutzrechtlichen Vorschriften, die Haftung des Verantwortlichen sowie Sanktionen gegen diesen.

Kapitel IV der DSRL befasst sich mit dem wichtigen Themenblock der Übermittlung personenbezogener Daten in Dritt- also Nicht-EU bzw. EEA-Länder. Infolge wachsender Technisierung und Globalisierung werden diese Vorschriften immer praxisrelevanter. Bei Datentransfers sind die Regelungen in Art. 25 und 26 DSRL zu berücksichtigen. Datenübermittlungen in Drittländer sind hiernach nur zulässig, sofern das Empfangsland ein angemessenes Schutzniveau gewährleistet oder eine der benannten Ausnahmen einschlägig ist. Eine Ausnahme liegt z.B. vor bei Einwilligung durch den Betroffenen oder aber sofern die Übermitt-

[360] EuGH, Urt. v. 09.03.2010, C-518/07 Kommission./.Deutschland, abrufbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=1083008 (04.04.2013).

lung zur Vertragserfüllung erforderlich ist, Art. 26 Abs. 1 a) und b) DSRL. Möglich ist auch die Übermittlung in ein Drittland ohne angemessenes Schutzniveau, sofern der Schutz der Privatsphäre, der Grundrechte und der Grundfreiheiten des Betroffenen vom für die Datenverarbeitung Verantwortlichen – insbesondere durch entsprechende Vertragsklauseln – garantiert wird, Art. 26 Abs. 2 DSRL. Hierunter fällt u.a. das *Safe-Harbor*-Abkommen mit den USA.[361]

Dieses bestehende Schutzkonzept plant der europäische Gesetzgeber nunmehr zu überarbeiten und insbesondere an die gewachsenen Herausforderungen der Datenverarbeitung infolge rascher technologischer Entwicklungen und der Globalisierung anzupassen.[362] Auch Entwicklungen im Bereich der RFID-Technologie werden in diesem Zusammenhang von der Kommission angeführt. So würden einerseits die Verfahren zur automatischen Erfassung personenbezogener Daten immer undurchsichtiger und gleichfalls die Bestimmung des Aufenthaltsorts einer Person immer einfacher, wie am Beispiel elektronischer Fahrausweise[363] und Straßengebührenerhebungen[364] deutlich wird.[365] Folgende Hauptziele für die Reformierung des europäischen Datenschutzrechts formuliert die Kommission:

Zunächst sollen die Rechte des Einzelnen umfassend gestärkt werden.[366] Hierzu gehört nicht nur die Nachbesserung im Bereich des Datenschutzes im Zusammenhang mit neuen Technologien[367] sondern auch die Förderung der Selbstverantwortung und Kontrolle durch Schaffung höherer Transparenz für die von der Verarbeitung Betroffenen.[368] Die Kommission plant u.a. die Erstellung von standardisierten EU-Datenschutzhinweisen ebenso wie eine allgemeine Anzeigepflicht für Datenschutzverstöße. Den Betroffenen soll zudem bessere Kontrolle über ihre Daten eingeräumt werden.[369] Hierbei soll das Prinzip der Datensparsamkeit gestärkt und das Recht auf Vergessen (*right to be forgotten*) präzisiert werden.[370] Weiterhin möchte die Kommission die Bestimmungen zur Einwilligung überprüfen und erörtern, wie diese insbesondere in der Online-Umgebung präzisiert und gestärkt werden können.[371] Die Kommission plant außerdem die Sondierung der Pflicht zu allgemeinen Aufklärungsmaßnahmen[372] sowie die Überprüfung spezieller Datenkategorien und ihre Bewertung als sensible Daten[373].

---

[361] Vgl. einführend *Klug*, RDV 2000, 212 ff.

[362] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 2.

[363] S.o. B.II.3.b).

[364] S.o. B.II.2.f).

[365] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 2.

[366] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 5.

[367] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 6.

[368] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 6 f.

[369] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 8 f.

[370] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 8.

[371] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 9 f.

[372] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 9.

[373] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 10.

Neben den Rechten des Einzelnen sollen auch die Binnenmarktdimensionen des europäischen Datenschutzes gestärkt werden.[374] Wesentliche Ansätze sind hierbei eine weitergehende Harmonisierung der Datenschutzbestimmungen in den Mitgliedstaaten[375], die Klärung der Bestimmungen über das anwendbare Recht und der Verantwortung der Mitgliedstaaten[376] sowie der Belegung des für die Verarbeitung Verantwortlichen mit mehr Verantwortung[377]. Spezifisch möchte die Kommission die verpflichtende Benennung eines unabhängigen Datenschutzbeauftragten einführen, Unternehmen, die mit risikobehafteter Datenverarbeitung betraut sind dazu verpflichten, eine Datenschutzfolgenabschätzung, insbesondere beim Einsatz bestimmter Technologien z.B. bei der Erstellung von Profilen, durchzuführen – hinsichtlich RFID-Anwendungen gibt es hierzu bereits Entwicklungen[378] – und überprüfen welche Maßnahmen zur Förderung des *Privacy-by-Design*-Konzepts ergriffen werden können.[379] Weiterhin verfolgt die Kommission Ansätze zur verstärkten Förderung von Initiativen zur Selbstregulierung und zur Einführung von EU-Zertifizierungsregelungen.[380]

Die Vorschläge der Kommission werden in einem nächsten Schritt dem Europäischen Parlament und dem EU-Ministerrat zur weiteren Erörterung vorgelegt. Sie sollen zwei Jahre nach dem Inkrafttreten, also frühestens 2014, zur Anwendung gelangen (Art. 91 des Verordnungsentwurfs) bzw. in nationales Recht umgesetzt sein (Art. 62 des Richtlinienentwurfs). Angesichts des sich regenden Widerstandes[381] gegen die geplanten Änderungen ist allerdings damit zu rechnen, dass ein Inkrafttreten der Vorschläge mit ihrem momentanen Inhalt – wenn überhaupt – noch geraume Zeit dauern dürfte, wodurch sich auch die Anwendung nach hinten verschieben wird.

b) Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG

Die eDSRL ergänzt die DSRL mit Regeln betreffend die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Aufgrund der Tatsache, dass die entsprechenden Vorschriften speziell auf Gefahren im Zusammenhang mit elektronischen Kommunikationsdiensten über das Internet ausgelegt sind, finden sie auf RFID-Szenarien nur Anwendung, sofern „solche Geräte an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder (…) elektronische Kommunikationsdienste

[374] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S.11 ff..

[375] Mitteilung der Kommission, KOM(2012) 9 endgültig, oben Fn. 356, S.7 ff.

[376] Mitteilung der Kommission, KOM(2012) 9 endgültig, oben Fn. 356, S.12.

[377] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 13 f.

[378] Vgl. hierzu unten E.II.1.a) sowie E.II.3.

[379] Mitteilung der Kommission, KOM(2012) 9 endgültig, oben 356, S. 4 ff.

[380] Mitteilung der Kommission, KOM(2010) 609, oben Fn. 357, S. 14 f.

[381] Vgl. nur Heise News Meldung vom 31.03.2012, Bundesrat stellt sich gegen geplante EU-Datenschutzreform, abrufbar unter http://www.heise.de/newsticker/meldung/Bundesrat-stellt-sich-gegen-geplante-EU-Datenschutzreform-1498251.html (04.04.2013); Heise News Meldung vom 07.03.2012, Oberster EU-Datenschützer greift Redings Reformpaket an, abrufbar unter http://www.heise.de/newsticker/meldung/Oberster-EU-Datenschuetzer-greift-Redings-Reformpaket-an-1465832.html (04.04.2013).

als Grundinfrastruktur genutzt“[382] werden. Artikel 3 der eDSRL wurde im Rahmen des Europäischen Telekom-Pakets von 2009[383] dahingehend geändert:

> Artikel 3 eDSRL Betroffene Dienste
>
> Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die **Datenerfassungs- und Identifizierungsgeräte unterstützen** [Hervorhebung eingef. d. Verf.].

Erwägungsgrund 56 der Änderungsrichtlinie 2009/136/EG präzisiert diese Formulierung dahingehend, dass RFID-Anwendungen, sofern sie an öffentliche Kommunikationsnetze angeschlossen sind, nunmehr vom Anwendungsbereich der eDSRL umfasst sein sollen.

> Erwägungsgrund 56 Richtlinie 2009/136/EG
>
> (…) Werden solche [RFID, eingef. d. Verf.] Geräte an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder werden elektronische Kommunikationsdienste als Grundinfrastruktur genutzt, so sollten die einschlägigen Bestimmungen der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), einschließlich der Vorschriften über Sicherheit, Datenverkehr, Standortdaten und Vertraulichkeit, zur Anwendung kommen.

Die Regelung wird indes für die meisten RFID-Anwendungen zu keiner neuen Bewertung führen. Die (telekommunikationsrechtlichen) Vorschriften gelten nämlich nur für die Anbieter des verwendeten öffentlich zugänglichen elektronischen Kommunikationsdienstes. Dieser wird regelmäßig der Internetzugangsanbieter (ISP) der datenverarbeitenden Stelle sein, der die im Rahmen einer RFID-Anwendung erhobenen Daten durch seine Netze leitet. Hierbei wird es auch kaum der Fall sein, dass das öffentliche Kommunikationsnetz des ISP die im Rahmen der RFID-Anwendung verwendeten Datenerfassungs- und Identifizierungsgeräte unterstützt. Dafür wäre im Zweifel eine enge Zusammenarbeit zwischen den ISP und den Betreibern von RFID-Systemen erforderlich. Eine solche zeichnet sich zum jetzigen Zeitpunkt nicht ab. Vielmehr dürfte die nahe Zukunft so aussehen, dass RFID-Anwender Daten im Rahmen ihrer RFID-Anwendung erheben, diese gegebenenfalls bereits verarbeiten (speichern, kombinieren u.a.) um sie dann unter Inanspruchnahme des Telekommunikationsdienstes des ISP – nämlich dem Internetzugang – durch das Netz des ISP an ihren Bestimmungsort zu transferieren.

c) Verhältnis von DSRL und eDSRL

Weil die eDSRL die DSRL ergänzt und im Verhältnis zu ihr *lex specialis* ist, muss im Einzelfall genau geprüft werden, welche der beiden Richtlinien Anwendung findet. Die Artikel-29

---

[382] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Erwägungsgrund 56, ABl. L 337 vom 18.12.2009, S. 11ff., abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:PDF (04.04.2013).

[383] Alle Rechtsakte abrufbar unter http://eur-lex.europa.eu/JOIndex.do?year=2009&serie=L&textfield2=337&Submit=Suche&_submit=Suche&ihmlang=de (04.04.2013).

Datenschutzgruppe hat in einem Arbeitspapier vom Dezember 2000[384] das Verhältnis der beiden herausgearbeitet.[385] Hiernach ist die DSRL immer dann anzuwenden, wenn die eDSRL keine spezielleren Regelungen beinhaltet so wie die Pflichten des für die Datenverarbeitung Verantwortlichen und die Rechte des Einzelnen sowie in Fällen von nicht-öffentlichen Telekommunikationsdiensten. Das bedeutet, dass die Richtlinien auch parallel Anwendung finden können. Wie gezeigt, kommt die eDSRL aber ohnehin nur zur Anwendung, wenn die verantwortliche Stelle auch gleichzeitig Anbieter des verwendeten Telekommunikationsdienstes ist.

II. Deutschland

Datenschutzrecht in Deutschland basiert auf dem durch das Grundgesetz gewährleisteten Recht auf informationelle Selbstbestimmung als besondere Ausformung des allgemeinen Persönlichkeitsrechts. Hierauf aufbauend finden sich datenschutzrechtliche Regelungen sowohl auf Landes- als auch Bundesebene. Diese Arbeit wird sich maßgeblich mit den Regelungen des BDSG auseinandersetzen und an den gegebenen Stellen auf Spezial- oder Landesgesetze hinweisen.

1. Grundgesetz – Recht auf Informationelle Selbstbestimmung

Verfassungsrechtliche Grundlage des Datenschutzes in Deutschland ist das allgemeine Persönlichkeitsrecht in seiner speziellen Ausformung des Rechts auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[386] Dies hat das BVerfG in seinem Volkszählungsurteil vom 15. Dezember 1983[387] verbindlich festgestellt. Das allgemeine Persönlichkeitsrecht in seiner speziellen Ausformung des Rechts auf informationelle Selbstbestimmung gewährt dem Einzelnen die Befugnis, „selbst über Preisgabe und Verwendung persönlicher Daten zu bestimmen“.[388]

Seine Grundlage findet das allgemeine Persönlichkeitsrecht in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Es bildet mit der allgemeinen Handlungsfreiheit zwei selbstständige sich aus Art. 2 Abs. 1 GG ergebende Grundrechte. Die allgemeine Handlungsfreiheit entfaltet sich hierbei in aktiver Weise[389], schützt also die freie Entscheidung über eigenes Tun oder Unterlassen i.S. einer Verhaltensfreiheit. Das allgemeine Persönlichkeitsrecht schützt demgegenüber in passiver oder statischer Weise die Privatsphäre. Der Einzelne genießt Schutz vor dem Zugriff auf die durch die Verhaltensfreiheit geschaffenen Tatbestände, so der Vertraulichkeit

---

[384] Artikel-29 Datenschutzgruppe, WP 37, Privatsphäre im Internet, vom 21. November 2000, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37de.pdf (04.04.2013).

[385] Zwar bezieht sich die Datenschutzgruppe auf Richtlinie 97/66/EG (die eDSRL war zu diesem Zeitpunkt noch gar nicht in Kraft) aber die getroffenen Aussagen sind auch auf die eDSRL anwendbar. Die eDSRL hat RL 97/66/EG abgelöst; so auch *Kuner*, European Data Protection Law, S. 27.

[386] *Starck* in: v. Mangoldt/Klein/Starck, GG I, Art. 2 Rn. 114, der den Terminus „informationelles Selbstbestimmungsrecht“ als unscharf beurteilt; *Jarass/Pieroth*, GG, Art. 2 Rn. 42 ff.

[387] BVerfGE 65, 1 – Volkszählung; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 141.

[388] BVerfGE 65, 1 (43) – Volkszählung; 84, 192 (194); 113, 29 (46).

[389] Andere verwendete Abgrenzungsbegriffe sind tun/sein, Aktus/Status, Aktivität/Integrität, *Kube*, Persönlichkeitsrecht *in*: HStR VII, 2009, § 148 Rn. 28.

des privaten Bereichs, insbesondere vor staatlicher Ausforschung ebenso wie vor verfälschender Darstellung („Daten“ über Lebensführung im weiten Sinne).[390]

Das allgemeine Persönlichkeitsrecht wurde erstmals durch das BVerfG in der sog. „Mikrozensus“-Entscheidung[391] anerkannt und fortan auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gestützt.[392] Art. 1 Abs. 1 GG ist hierbei als programmatische Leit- und Ausgestaltungsrichtlinie zu verstehen und nicht als eigentlich betroffene Norm. Ansonsten wären – wegen des vorbehaltlosen Schutzes der Menschenwürde – durchaus gewollte Einschränkungen des allgemeinen Persönlichkeitsrechts nicht möglich.[393] Basisnorm des allgemeinen Persönlichkeitsrechts ist damit Art. 2 Abs. 1 GG; Art. 1 Abs. 1 GG wirkt gewährleistungsverdeutlichend und –intensivierend.[394]

Im Verhältnis zu anderen, die konstituierenden Elemente der Persönlichkeit schützenden Grundrechten (Gewissensfreiheit, Meinungsäußerungsfreiheit, Berufsfreiheit, Eigentumsfreiheit, Brief-, Post- und Fernmeldegeheimnis), verhält sich das allgemeine Persönlichkeitsrecht als Auffanggrundrecht.[395]

a) Schutzbereich

Geschützt wird durch das allgemeine Persönlichkeitsrecht einerseits die *Selbstentfaltung* durch Abschirmung eines privaten Bereichs und andererseits die nach außen gerichtete *Selbstdarstellung* vor verfälschender, entstellender oder einfach nur unautorisierter Präsentation der eigenen Person in der Öffentlichkeit.[396]

Angesichts der sich stetig wandelnden Gefährdungslagen – insbesondere durch die sich rapide entwickelnde Informationsstrukturen – wurden vom BVerfG verschiedene Ausformungen des allgemeinen Persönlichkeitsrechts herausgebildet. Das *Recht auf informationelle Selbstbestimmung* als Grundlage des Datenschutzes ist eine dieser speziellen Ausformungen, das jedenfalls terminologisch Selbstständigkeit erfährt[397].

Erstmals setzte sich das BVerfG in seinem „Volkszählungsurteil“[398] mit dem Recht auf informationelle Selbstbestimmung auseinander. Normativ war dies seine Geburtsstunde. Es ist folglich auch jünger als das erste BDSG (dieses trat am 01.01.1979 in Kraft) und die Datenschutzgesetze der Länder (Hessen verabschiedete 1970 das erste Datenschutzgesetz[399] welt-

---

[390] *Dreier*, GG Art. 2 I Rn. 23; *Kube*, Persönlichkeitsrecht *in*: HStR VII, 2009, § 148 Rn. 28.

[391] BVerfGE 27, 1 (6f.).

[392] St. Rspr. BVerfGE 35, 202 (219); 72, 155 (170); 82, 236 (269); 90, 263 (270); *Dreier*, GG Art. 2 I Fn. 260 m.w.N.

[393] *Dreier*, GG Art. 2 I Rn. 68.

[394] *Kube*, Persönlichkeitsrecht *in*: HStR VII, 2009, § 148 Rn. 32.

[395] *Kube*, Persönlichkeitsrecht *in*: HStR VII, 2009, § 148 Rn. 34 f.

[396] *Dreier*, GG Art. 2 I Rn. 69; *Kube*, Persönlichkeitsrecht *in*: HStR VII, 2009, § 148 Rn. 37.

[397] *Kunig* in: v. Münch/Kunig, GG, Art. 2 Rn. 38.

[398] BVerfGE 65, 1 (41ff.) – Volkszählung.

[399] GVBl. I 1970 S. 625.

weit). Dennoch basiert der einfachgesetzlich normierte Datenschutz heute auf dem Recht auf informationelle Selbstbestimmung und dient gleichzeitig seiner Absicherung[400]. In jüngerer Zeit hat das BVerfG zwei weitere für den Datenschutz wichtige Entscheidungen erlassen. Dies waren zum einen das Urteil zur Vorratsdatenspeicherung[401] und zum anderen die Entscheidung zur Online-Durchsuchung[402]. In letzterem Urteil hat das BVerfG erstmals das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme anerkannt[403], welches eine der weiteren Ausformungen des allgemeinen Persönlichkeitsrechts ist.[404]

Das Recht auf informationelle Selbstbestimmung umfasst die Befugnis des Einzelnen, selbst zu entscheiden, wann und wem er zu welchem Zweck personenbezogene Daten offenbart. Das BVerfG hierzu im Volkszählungsurteil:

> „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[405]

Durch den Schutz vor unautorisierter oder auch nur unbemerkter Erhebung oder Verarbeitung personenbezogener Daten durch einen Dritten, soll verhindert werden, dass der Einzelne „in seiner Freiheit wesentlich gehemmt wird, aus eigener Selbstbestimmung zu planen oder zu entscheiden“[406]. Damit wird das informationelle Selbstbestimmungsrecht zur Grundlage der Persönlichkeitsentwicklung und Persönlichkeitsentfaltung.[407] In einer neueren Entscheidung spricht das BVerfG ausdrücklich vom „grundrechtlichen Datenschutz“[408], was teilweise als Formulierung des „Grundrechts auf Datenschutz“ interpretiert wurde.[409] Eine spezielle Normierung hat dieses Grundrecht auf Datenschutz im Grundgesetz indes bis heute nicht erfahren.

Der sachliche Schutzbereich bestimmt sich maßgeblich über den Begriff der personenbezogenen Daten, der zugleich über die Anwendbarkeit der Datenschutzgesetze entscheidet. Was

---

[400] *Roßnagel* in: Roßnagel, HdB DSR, 1. Einleitung, Rn. 4.

[401] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, BVerfGE 125, 260, oben Fn. 328 – Vorratsdatenspeicherung.

[402] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, abrufbar unter http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (04.04.2013) = BVerfGE 120, 274 – Online Durchsuchung.

[403] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, oben Fn. 402 – Online Durchsuchung, 1. Leitsatz.

[404] Mehr hierzu unten D.II.1.c).

[405] BVerfGE 65, 1 (43) – Volkszählung.

[406] BVerfGE 65, 1 (43) – Volkszählung.

[407] *Roßnagel* in: Roßnagel, HdB DSR, 1. Einleitung, Rn. 4.

[408] BVerfG NJW 1991, 2129 (2132).

[409] So Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, Einleitung, Rn. 16; kritisch *Di Fabio* in: Maunz/Dürig, GG, Art. 2 Rn. 173.

personenbezogene Daten sind, ist einfachgesetzlich definiert. Auf Bundesebene ist die Definition des BDSG maßgebend.

> § 3 Abs. 1 BDSG
>
> Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Der Schutzbereich des Grundrechts geht aber zugleich über den Anwendungsbereich des einfachgesetzlichen Datenschutzrechts hinaus. Während letzteres lediglich personenbezogene Daten zum Gegenstand hat, bezieht sich das Grundrecht auch auf bloße Informationen. Das Datum unterscheidet sich zur Information dadurch, dass es in irgendeiner Weise perpetuiert ist.[410]

Persönlich unterfallen dem Schutzbereich nur natürliche Personen. Personenbezogene Daten können zwar auch in der Hand juristischer Personen sein. Geschützt wird aber der Schutz der Daten einer natürlichen Person – des Datensubjekts – und nur diese kann sich auf das Grundrecht berufen. Dies gilt auch, wenn die Daten in der Hand eines Dritten – auch einer juristischen Person – sind, der die Daten schützen möchte.[411]

b) Schranken

Das Recht auf informationelle Selbstbestimmung ist trotz seiner Nähe zu Art. 1 Abs. 1 GG nicht vorbehaltlos gewährleistet. Staatliche Eingriffe sind vielmehr aufgrund entsprechender Ermächtigungsgrundlage möglich. Die Rechtfertigung solcher Eingriffe richtet sich nach den Schranken des Art. 2 Abs. 1, 2. Hs. GG – der sog. Schrankentrias.[412] Das BVerfG legt hierbei allerdings im Vergleich zu Beschränkungen der allgemeinen Handlungsfreiheit strengere Maßstäbe an, indem es den Begriff der „verfassungsmäßigen Ordnung“ – welcher einen einfachen Gesetzesvorbehalt beschreibt[413] – dahingehend beschränkt, dass es förmliche Gesetze für die Rechtfertigung von Eingriffen in das informationelle Selbstbestimmungsrecht verlangt.[414] Ein solches förmliches Gesetz muss zudem einem überwiegenden Allgemeininteresse dienen, verhältnismäßig sein und dem Gebot der Normenklarheit entsprechen.[415]

Teilweise wird angenommen das allgemeine Persönlichkeitsrecht unterfalle in Bezug auf die Beschränkbarkeit Art. 1 Abs. 1 GG und nicht Art. 2 Abs. 1 GG.[416] Wendete man diese Interpretation auch auf das Recht auf informationelle Selbstbestimmung an, führte dies – infolge

---

[410] *Schmitt Glaeser*, Schutz der Privatsphäre in: HStR VI, 1989, § 129 Rn. 77 f. m.w.N.

[411] *Schmitt Glaeser*, Schutz der Privatsphäre in: HStR VI, 1989, § 129 Rn. 88.

[412] BVerfGE 65, 1 (44) – Volkszählung; dies sieht im Ergebnis ebenso *Tiedemann*, DÖV 2003, 74 (77), der allerdings das Recht auf informationelle Selbstbestimmung nicht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG ableitet sondern es nur als Recht aus Art. 2 Abs. 1 GG ansieht.

[413] *Di Fabio* in: Maunz/Dürig, GG, Art. 2 Rn. 133, m.w.N.

[414] *Dreier* in: Dreier, GG, Art. 2 I Rn. 86; *Kunig* in: v. Münch/Kunig, Art. 2 Rn. 42; BVerfGE 65, 1 (44) – Volkszählung.

[415] *Fassbender*, Wissen als Grundlage staatlichen Handelns *in*: HStR IV, 2006, § 76 Rn. 66; Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, Einleitung, Rn. 19.

[416] So Tiedemann, DÖV 2003, 74 (76).

der vorbehaltlos gewährten Menschenwürde – dazu, dass Eingriffe nicht gerechtfertigt werden könnten. Eine derartige Überdehnung des Rechts auf informationelle Selbstbestimmung war hingegen vom BVerfG nicht gewollt.[417] Die Menschenwürdegarantie bestimmt also den Inhalt und die Grenzen des allgemeinen Persönlichkeitsrechts mit, die Rechtsfolge der Unantastbarkeit ist hingegen nicht anzuwenden.[418]

Vielmehr sind die Schranken nach den allgemeinen Grundsätzen – insbesondere dem Grundsatz der Verhältnismäßigkeit – durch die sog. Schranken-Schranken zu begrenzen. Im Volkszählungsurteil führt das BVerfG bezüglich des informationellen Selbstbestimmungsrechts hierzu aus:

> „Bei seinen Regelungen [zu den Beschränkungen; eingef. d. Verf.] hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerlässlich ist. Angesichts der bereits dargelegten Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“[419]

Zu berücksichtigende Aspekte bei der Anwendung des Verhältnismäßigkeitsprinzips sind die Art der Daten, die Art der Erhebung und der Benutzung der Daten in ihren verschiedenen Varianten.[420]

Nach der vom BVerfG zum allgemeinen Persönlichkeitsrecht entwickelten „Sphärentheorie“ sollen Eingriffe in den Bereich des als „Intimsphäre“ bezeichneten Kernbereichs der Persönlichkeitsgestaltung nicht zu rechtfertigen sein.[421] Für das Recht auf Informationelle Selbstbestimmung hat das BVerfG aber Abstand von der Sphärentheorie genommen[422]:

> „(…) insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung **kein "belangloses" Datum** [Hervorhebung eingef. d. Verf.] mehr. Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.“[423]

Aus dem Bezug zu der in Art. 1 Abs. 1 S. 1 GG geschützten Menschenwürde ergibt sich, dass auch ohne Einbeziehung der Sphärentheorie der Eingriff in den „letzten unantastbaren Bereich privater Lebensgestaltung“[424] nicht zu rechtfertigen. Je intimer die Angaben sind, die

---

[417] *Dreier*, GG Art. 2 I Rn. 86.

[418] *Kube*, Persönlichkeitsrecht *in*: HStR VII, 2009, § 148 Rn. 83.

[419] BVerfGE 65, 1 (44) – Volkszählung.

[420] *Starck* in: v. Mangoldt/Klein/Starck, GG I, Art. 2 Abs. 1 Rn. 119; BVerfGE 65, 1 (46) – Volkszählung.

[421] BVerfGE 6, 32 (41) – Elfes; *Dreier*, GG Art. 2 I Fn. 359.

[422] Vgl. hierzu *Kunig* in: v. Münch/Kunig, GG, Art. 2 Rn. 41.

[423] BVerfGE, 65, 1 (45) – Volkszählung.

[424] Erstmals formuliert in BVerfGE 6, 32 (36) – Elfes.

der Betroffene machen soll,[425] oder je mehr die Verwendung der Daten geeignet ist, Totalabbilder von Persönlichkeitsprofilen zu erstellen,[426] desto gewichtiger muss auch das öffentliche Interesse an der Datenerhebung sein. Fällt die Abwägung nicht zu Gunsten des öffentlichen Interesses aus, ist die Datenerhebung nicht mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar.

Das eingreifende Gesetz muss auch bezüglich des Bestimmtheitsgrundsatzes erhöhte Anforderungen erfüllen. Hierzu das BVerfG:

> „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck **bereichsspezifisch und präzise bestimmt** [Hervorhebung eingef. d. Verf.] und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren.“[427]

Vor dem Hintergrund des objektiv-rechtlichen Gehalts des informationellen Selbstbestimmungsrechts wurden mit dem Volkszählungsurteil prozedurale und organisatorische Vorkehrungen, die Missbrauchsmöglichkeiten ausschließen sowie Aufklärungs-, Auskunfts- und Löschungspflichten zum programmatischen Auftrag für den Gesetzgeber.[428]

Diese Einschätzung hat das BVerfG zuletzt in seinem Urteil zur Vorratsdatenspeicherung[429] bestätigt. Zwar hielt es hier das Recht auf informationelle Selbstbestimmung nicht für einschlägig, allerdings sei das grundrechtlich in Art. 10 GG geschützte Fernmeldegeheimnis als spezielle Garantie anzuwenden.[430] Die für das Recht auf informationelle Selbstbestimmung entwickelten Grundsätze konnten daher auch weitgehend auf das Fernmeldegeheimnis übertragen werden. Mit dem Urteil wurden die §§ 113a und b TKG gänzlich für nichtig erklärt, die eine anlasslose Speicherung aller Internetverkehrsdaten durch die Internetserviceanbieter für einen Zeitraum von sechs Monaten vorsahen. § 100g Abs. 1 S. 1 StPO wurde insoweit für nichtig erklärt, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften. Bei der Vorratsdatenspeicherung handelt es sich um eine staatlich veranlasste Speicherung und unterscheidet sich damit von der Sammlung von RFID-Daten durch die Wirtschaft, die rein ökonomische Ziele verfolgt. Bei staatlich veranlassten Datensammlungen sind, darauf weist das BVerfG ausdrücklich hin, andere Maßstäbe anzuwenden, als bei durch privatwirtschaftliche Unternehmen veranlasster Datensammlung:

---

[425] BVerfGE 65, 1 (46).

[426] *Schmitt Glaeser* in: HStR IV, 1989, § 129 Rn. 45.

[427] BVerfGE 65, 1 (46) – Volkszählung.

[428] *Di Fabio* in: Maunz/Dürig, GG Art. 2 Rn. 177 f.

[429] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, BVerfGE 125, 260, oben Fn. 328 – Vorratsdatenspeicherung.

[430] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 191 = BVerfGE 125, 260 (310), oben Fn. 328 – Vorratsdatenspeicherung.

> „Allerdings entspricht es der ständigen Rechtsprechung des Bundesverfassungsgerichts, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist.[431] […]
>
> Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG speichern dürfen.[432] […]“

Das Urteil erstreckte sich auf die Speicherung sämtlicher Telekommunikationsverbindungsdaten auf Vorrat zur Bekämpfung von Straftaten. Die Dinge liegen bereits aus dem Grunde anders als bei – insbesondere primär produktbezogenen – RFID-Daten, weil hier die speichernde Stelle anders als bei der Vorratsdatenspeicherung der Telekommunikationsanbieter, der den betreffenden Telefonnummern oder IP-Adressen soziale Identifikatoren wie den Namen zuordnen kann, regelmäßig keine unmittelbare Verbindung zwischen den betreffenden produktbezogenen EPC- oder sonstigen Identifikationsnummern und konventionellen personenbezogenen Daten der sie bei sich führenden Person herstellen kann.

Nichts desto trotz sind die allgemeinen Ausführungen des BVerfG zum Gefahrpotenzial umfassender Speicherungen von Telekommunikationsverbindungsdaten wegweisend und haben auch maßgeblichen Einfluss auf die Bewertung der durch RFID hervorgerufenen datenschutzrechtlichen Herausforderungen. Die durch die Allgegenwärtigkeit der Datensammlung hervorgerufene besondere Schwere des Eingriffs in die Rechte der Betroffenen – namentlich aller Bürger –, auf die das BVerfG mehrfach hinweist,

> „Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer **Streubreite, wie sie die Rechtsordnung bisher nicht kennt** [Hervorhebung eingef. d. Verf.]: Erfasst werden über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine - auch nur abstrakte - Gefährlichkeit oder sonst eine qualifizierte Situation. Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist.“[433] […]

ist jedenfalls insofern vergleichbar mit Datenspeicherungen in einer Welt ubiquitärer RFID-Anwendungen, als auch hier das Potenzial besteht, alle RFID-Daten immerwährend und flächendeckend zu erfassen, womit ebenfalls sämtliches Alltagshandeln umfasst wäre, ohne dass sich die Bürger dieser Struktur noch entziehen könnten.

Die drohende Gefahr eines solchen von den Betroffenen unbemerkten Sammelverhaltens, nämlich das Gefühl ständigen Überwachtseins, erkennt auch das BVerfG:

> […] „Besonderes Gewicht bekommt die Speicherung der Telekommunikationsdaten weiterhin dadurch, dass sie selbst und die vorgesehene Verwendung der gespeicherten Daten von den Betroffenen unmittelbar nicht bemerkt werden, zugleich aber Verbindungen erfassen, die unter Vertraulichkeitserwartungen aufgenommen werden. Hierdurch ist die anlasslose Speicherung von Telekommunikationsver-

[431] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 213 = BVerfGE 125, 260 (321), oben Fn. 328 – Vorratsdatenspeicherung.

[432] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 227 = BVerfGE 125, 260 (328), oben Fn. 328 – Vorratsdatenspeicherung.

[433] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 209 = BVerfGE 125, 260 (318), oben Fn. 328 – Vorratsdatenspeicherung.

> kehrsdaten geeignet, ein **diffus bedrohliches Gefühl des Beobachtetseins** [Hervorhebung eingef. d. Verf.] hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann."[434]

Auch auf die Gefahr der Anlegung umfassender Persönlichkeits- und Bewegungsprofile weist das BVerfG hin:

> „Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst - und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen - tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. Zwar werden mit einer Telekommunikationsverkehrsdatenspeicherung […] nur die Verbindungsdaten […] festgehalten […]. Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten […], Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die **Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers** [Hervorhebung eingef. d. Verf.] ermöglichen."[435] […]

Vergleichbare Profile können – wie oben gesehen – auch mittels RFID-Daten erstellt werden, wenn sie nur hinreichend lange und umfassend erfasst und ausgewertet werden.

Vor dem Hintergrund, dass es sich bei der Vorratsdatenspeicherung um eine staatlich veranlasste Datensammlung handelt, stellt das BVerfG fest, dass Gesetze, die hierzu ermächtigen sollen,

> […] „besonderen verfassungsrechtlichen Anforderungen insbesondere hinsichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes"[436] […]

unterliegen. Mangels staatlicher Veranlassung gelten für die Sammlung von RFID-Daten andere Maßstäbe und die Forderungen des BVerfG die Vorratsdatenspeicherung betreffend können nicht ohne weiteres übertragen werden. Damit bleibt es zunächst bei den allgemeinen Anforderungen an Datensicherheit, Zweckbindung, Erforderlichkeit, Betroffeneninformation sowie Betroffenenrechte, wie bereits im Volkszählungsurteil gefordert und im BDSG umgesetzt. Möglicherweise ist aber mit dem BVerfG ebenso wie bei der Vorratsdatenspeicherung

> „**Das Fehlen hinreichender Sicherheitsstandards** im Telekommunikationsgesetz **kann auch § 9 BDSG in Verbindung mit der zugehörigen Anlage nicht ausgleichen** [Hervorhebung eingef. d. Verf.]. Unbeschadet ihrer zum Teil abstrakt hohen Standards bleibt diese Norm, die ohnehin nur subsidiär anwendbar ist […], zu allgemein, um in hinreichend spezifischer und verlässlicher Weise die besonders hohen Sicherheitsstandards bezüglich der nach § 113a TKG zu speichernden Daten sicherzustellen."[437]

---

[434] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 212 = BVerfGE 125, 260 (320), oben Fn. 328 – Vorratsdatenspeicherung.

[435] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 211 = BVerfGE 125, 260 (319), oben Fn. 328 – Vorratsdatenspeicherung.

[436] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 220 = BVerfGE 125, 260 (325), oben Fn. 328 – Vorratsdatenspeicherung.

[437] BVerfG Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 274 = BVerfGE 125, 260 (350 f.), oben Fn. 328 – Vorratsdatenspeicherung.

auch für RFID-Anwendungen und die zugrunde liegenden Gesetze – heute also maßgeblich das BDSG – ein spezifischer Schutz zu fordern, der über die bestehenden Regelungen hinausgeht bzw. diese anwendungsspezifisch ersetzt.

c) Verhältnis zum Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Am 27. Februar 2008 hat das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts mit Datenschutzrelevanz herausgebildet: Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[438] Dieses IT- oder Computergrundrecht genannte Recht

> „schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist.“[439]

Damit ist für RFID-Anwendungen eine Abgrenzung der jeweiligen Anwendungsbereiche – maßgeblich zum Recht auf informationelle Selbstbestimmung – vorzunehmen, wobei das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme subsidiär gegenüber anderen Grundrechten ist. Das BVerfG führt hierzu aus:

> „Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert.“[440]

Auslegungsschwierigkeiten ergeben sich hierbei hinsichtlich mehrerer vom BVerfG verwendeter Begriffe, für das es keine Definition vorgibt. Zum einen ist nicht eindeutig, was als informationstechnisches System zu qualifizieren ist. Das BVerfG nennt hier beispielhaft Personalcomputer, Mobiltelefone und elektronische Terminkalender, weil diese über einen großen Funktionsumfang verfügten und personenbezogene Daten vielfältiger Art erfassen und speichern könnten.[441] Ob RFID-Systeme ebenfalls in den Anwendungsbereich fallen können, ist gerichtlich ungeklärt. Es wird vertreten, dies sei insofern der Fall, als auf RFID-Tags Daten gespeichert würden, die mittels Funkwellen an Lesegeräte übertragen werden könnten.[442] Unter Zugrundelegung eines Definitionsvorschlags des Bundesinnenministeriums ließe sich diese Schlussfolgerung in der Tat begründen. Das BMI fasst unter den Begriff alle Systeme, die aus Hard- und Software sowie aus Daten bestehen und die der Erfassung, Speicherung, Ver-

---

[438] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, oben Fn. 402 – Online Durchsuchung, 1. Leitsatz.

[439] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 167 = BVerfGE 120, 274 (302), oben Fn. 402 – Online Durchsuchung.

[440] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 200 = BVerfGE 120, 274 (312 f.), oben Fn. 402 – Online Durchsuchung.

[441] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 203 = BVerfGE 120, 274 (314), oben Fn. 402 – Online Durchsuchung.

[442] *Holznagel/Schumacher*, MMR 2009, 3 (4).

arbeitung, Übertragung und Anzeige von Informationen und Daten dienen.[443] Diese Vorgaben des Bundesinnenministeriums haben aber freilich keine verfassungsrechtliche Bindungswirkung und können allenfalls als Orientierungshilfe herangezogen werden.[444] Ob RFID-Systeme – und wenn ja, welche – grundsätzlich allein ihrer technischen Ausrichtung nach in den Schutzbereich des IT-Grundrechts fallen können, bleibt abschließend einer Entscheidung des BVerfG vorbehalten. Das BVerfG stellt weiterhin klar, dass nicht jedes informationstechnische System unter den Schutzbereich des IT-Grundrechts fällt:

> „Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält […] unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren.“[445]

Erfasst werden mithin solche Systeme,

> „[…] die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.“[446]

Die Abgrenzung zum Recht auf informationelle Selbstbestimmung erfolgt damit im Wesentlichen anhand des Kriteriums der Quantität: Geschützt werden nicht einzelne Daten – mit punktuellem Bezug zu einem bestimmten Lebensbereich – des Betroffenen sondern Datensammlungen, die in einem informationstechnischen System gespeichert und genutzt werden.[447]

Diese Datensammlungen müssen dem informationstechnischen System von dem Betroffenen anvertraut bzw. ihm durch seine bloße Nutzung geliefert werden.[448] Weiterhin muss ein Zugriff auf die in dem informationstechnischen System enthaltenen Daten geeignet sein, einen Einblick in wesentliche Teile der Lebensgestaltung des Betroffenen zu ermöglichen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.

Teilweise wird vertreten, Systeme, die Daten eigenständig sammeln und speichern, ohne dass der Nutzer diese herausgibt, seien nicht vom IT-Grundrecht erfasst.[449] Damit fielen alle EPC-

---

[443] Bundesministerium des Innern, Antworten auf den Fragenkatalog des Bundesministeriums der Justiz zur Online-Durchsuchung, vom 22.10.2007, abrufbar unter http://asset.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (04.04.2013), S. 2.

[444] So auch *Holznagel/Schumacher*, MMR 2009, 3 (4).

[445] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 202 = BVerfGE 120, 274 (313 f.), oben Fn. 402 – Online Durchsuchung.

[446] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 203 = BVerfGE 120, 274 (314), oben Fn. 402 – Online Durchsuchung.

[447] Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 31.

[448] BVerfG Urteil vom 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 200 = BVerfGE 120, 274 (313), oben Fn. 402 – Online Durchsuchung.

[449] *Holznagel/Schumacher*, MMR 2009, 3 (4).

Szenarien aus dem Schutzbereich des IT-Grundrechts heraus, weil in den betroffenen Einzelhandelsanwendungen der Betroffene das RFID-Tag bereits inklusive aller Daten, die auf ihm gespeichert sind, über den Kauf des zugehörigen Produkts erlangt; er vertraue damit dem System keinerlei Daten an.[450] Diese Ansicht setzt sich indes nicht weiter mit der Tatsache auseinander, dass nach dem Ergreifen der getaggten Produkte Auslesevorgänge in den Geschäftsräumen des Systembetreibers stattfinden (können), dass der Betroffene dem System also durch bloßes Beisichführen der getaggten Produkte Bewegungsdaten über sich preisgibt bzw. diesem zwangsläufig liefert.

Die gesammelten Daten müssen mit dem BVerfG weiterhin geeignet sein, einen Einblick in wesentliche Teile der Lebensgestaltung des Betroffenen zu ermöglichen. Eine pauschale Bewertung von RFID-Systemen hinsichtlich dieses Erfordernisses ist ausgeschlossen; zu unterschiedlich sind die verarbeiteten Daten, vgl. nur die herausgearbeiteten *Leading Scenarios*. Die Quantität der Daten spielt hier eine entscheidende Rolle: Während Daten einer bestimmten Qualität – z.B. sensible Daten i.S.d. § 3 Abs. 9 BDSG – bereits bei Vorliegen einer einzigen Information geeignet sind, Einblicke in wesentliche Teile der Lebensgestaltung des Betroffenen zu ermöglichen, ist dies bei Daten mit wenig Aussagekraft bzw. solchen, die ihrem Ursprung nach keinen Personenbezug aufwiesen – so wie EPC-Identifikationsnummern auf Produkt-RFIDs – anders zu bewerten. Die Möglichkeit des Einblicks in wesentliche Teile der Lebensgestaltung des Betroffenen bei produktbezogenen Identifikationsnummern von vornherein auszuschließen[451], ist allerdings verfehlt: Die oben dargestellten Herausforderungen von Tracking- und Profiling stellen sich gerade in diesem Bereich – und zwar auch ohne, dass der Betroffene durch Verknüpfung der Produktidentifikationsnummern mit weiteren Daten namentlich oder über sonstige konventionelle personenbezogene Daten eindeutig identifizierbar wäre. Verneinte man hier die Erheblichkeit potenzieller Beeinträchtigungen bereits auf Schutzbereichsebene, würde man in unzulässiger und unbegründeter Weise den vom BVerfG verfolgten Schutz verkürzen.

Aber auch bei RFID-Tags, auf denen konventionelle personenbezogene Daten gespeichert sind, ist die Möglichkeit des Einblicks in wesentliche Teile der Lebensgestaltung des Betroffenen nicht automatisch gegeben. Hier kommt es maßgeblich auf die Qualität der Daten an.[452]

Unterschiede zum Recht auf informationelle Selbstbestimmung ergeben sich hinsichtlich der Schutzrichtung des IT-Grundrechts auch in folgender Hinsicht: Während das Recht auf informationelle Selbstbestimmung die personenbezogenen Daten des Betroffen schützt, zielt das IT-Grundrecht auf die Vertraulichkeit und Integrität des informationstechnischen Systems ab, in dem die Daten gespeichert sind bzw. verarbeitet werden. Weil das informationstechnische System nicht zwangsläufig im Eigentum des Betroffenen stehen muss – geschützt wer-

[450] *Holznagel/Schumacher*, MMR 2009, 3 (4).

[451] So *Holznagel/Schumacher*, MMR 2009, 3 (5).

[452] *Holznagel/Schumacher*, MMR 2009, 3 (6) vertreten indes auch hier pauschal, dass der Schutzbereich des IT-Grundrechts nicht eröffnet sei, vielmehr auf das Recht auf informationelle Selbstbestimmung zurückzugreifen sei.

den wohl auch Daten, die der Betroffene fremden Systemen anvertraut, z.B. einem virtuellen Speicher in der Cloud – dürften die Daten als solche nicht gegen missbräuchliches Verhalten durch den Systembetreiber – also gegen missbräuchliches Verhalten „von innen" – geschützt sein.[453] Der Schutz dürfte sich damit lediglich auf Angriffe auf das System und die Daten von außen erstrecken. Die Tracking- und Profilinggefahren durch den Systembetreiber werden nach hier vertretener Ansicht mithin nicht vom IT-Grundrecht adressiert.

d) Wirkung des Informationellen Selbstbestimmungsrechts

Grundrechte sind primär Abwehrrechte gegen den Staat; in dieser Funktion wirken sie als subjektiv-öffentliche Unterlassungsansprüche.[454] Sie bestimmen in ihrem Schutzbereich und ihren Schranken, ob und wenn ja wie weit staatliches Verhalten in grundrechtlich geschützte Verhaltensweisen und Positionen des Einzelnen eingreifen darf. Private sind damit grundsätzlich nicht Adressaten der Grundrechte.

Zwischen Privaten gelten die Grundrechte nicht unmittelbar. Im Wege einer Ausstrahlung entfalten die Grundrechte allerdings zum einen mittelbare Drittwirkung[455]. Die einfache Rechtsordnung – also auch alle Gesetze, die das Verhältnis Privater untereinander regeln – ist durch alle staatliche Gewalt (Art. 1 Abs. 3 GG) und damit zuletzt den entscheidenden Richter im Lichte der Grundrechte auszulegen. Geschieht dies nicht, kann ein ungerechtfertigter Eingriff in die Grundrechte vorliegen, der mittels Verfassungsbeschwerde vor dem BVerfG überprüfbar ist.[456] Das informationelle Selbstbestimmungsrecht ist damit ebenso wie alle anderen Grundrechte bei staatlichen Maßnahmen zu berücksichtigen.

Die Schutzdimension der Grundrechte beinhaltet zudem die Pflicht des Staates, grundrechtlich verbürgte Verhaltensweisen und Positionen des Einzelnen effektiv durch Schaffung einfachgesetzlicher Normen zu schützen. Für das informationelle Selbstbestimmungsrecht heißt das, dass der Staat verpflichtet ist, „dem Einzelnen Schutz davor zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf die seine Individualität kennzeichnenden Daten nehmen"[457]. Dies gilt immer dann, wenn das Grundrecht besonders gefährdet ist, weil die Machtverhältnisse zwischen den privaten Partnern ungleich verteilt sind.[458] Im Hinblick auf das allgemeine Persönlichkeitsrecht in all seinen Ausformungen ist hierbei der besondere Wertgehalt von Art. 1 Abs. 1 GG zu berücksichtigen. Der Einfluss der Menschenwürdegarantie auf das allgemeine Persönlichkeitsrecht verpflichtet den Gesetzgeber, sich im

---

[453] Ähnlich auch *Holznagel/Schumacher*, MMR 2009, 3 (7), die den Schutz davon abhängig machen, dass der Betroffene das System „als eigenes nutzt und deshalb den Umständen nach davon ausgeben darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt".

[454] *Ossenbühl*, Grundsätze der Grundrechtsinterpretation *in*: HGR I, 2004, § 15 Rn. 45 f.

[455] Anerkannt durch die Rspr. des BVerfG zuerst in dessen „Lüth"-Urteil von 1958, BVerfGE 7, 198.

[456] *Di Fabio* in: Maunz/Dürig, GG Art. 2 Rn. 134.

[457] BVerfGE 117, 202 (229) – Vaterschaftsfeststellung; vgl. auch BVerfG Beschl. v. 23.10.2006 – 1 BvR 2027/02, abrufbar unter http://www.bundesverfassungsgericht.de/entscheidungen/rk20061023_1bvr202702.html (04.04.2013) – Versicherungsvertragliche Obliegenheit zur Schweigepflichtentbindung.

[458] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 154.

Zweifel auch auf Kosten grundrechtlich geschützter Rechte Dritter im Wege einfachgesetzlicher Ausgestaltung schützend vor das allgemeine Persönlichkeitsrecht zu stellen. Dies muss so sein, weil Beeinträchtigungen des Persönlichkeitsrechts in seiner Ausformung als informationelles Selbstbestimmungsrecht in Zeiten der Technisierung und Vernetzung zunehmend durch Private hervorgerufen werden und regelmäßig einseitige Machverhältnisse vorliegen.[459] Hieraus ergibt sich ein immerwährender Handlungsauftrag an den Gesetzgeber das informationelle Selbstbestimmungsrecht des Einzelnen im Bedarfsfall effektiv durch Schaffung neuer oder Anpassung bestehender einfachgesetzlicher Normen zu schützen.

Der Gesetzgeber ist diesem Handlungsauftrag durch Schaffung einerseits allgemeiner (BDSG, LDSGe) und andererseits bereichsspezifischer datenschutzrechtlicher Vorschriften (z.B. TKG, TMG) nachgekommen. Der Wandel in Gesellschaft und Technik macht allerdings regelmäßige Anpassungen notwendig.

Im Umkehrschluss verpflichtet die Schutzdimension des informationellen Selbstbestimmungsrechts auch dazu, dass der Gesetzgeber bei Schaffung von in selbiges eingreifender Regelungen (also insbesondere solcher, die datenverarbeitenden Stellen Zugriff auf und Verwendung von personenbezogenen Daten erlauben), dessen Gehalt zu bewahren hat.

2. Bundesdatenschutzgesetz (BDSG)

Die Umsetzung der europa- und verfassungsrechtlichen Vorgaben zum Datenschutz findet in Deutschland sowohl in vertikaler als auch in horizontaler Hinsicht auf verschiedenen Ebenen statt.[460] Zum einen ist zu unterscheiden zwischen der Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) auf der einen und der Landesdatenschutzgesetze auf der anderen Seite. Zum anderen finden sich datenschutzrechtliche Regelungen auch in Spezialgesetzen, so z.B. auf Bundesebene im Telekommunikationsgesetz (TKG) sowie im Telemediengesetz (TMG) und auf Landesebene in den Polizeigesetzen oder auch dem Rundfunkstaatsvertrag (RStV) sowie den Pressegesetzen. Das Bundesdatenschutzgesetz ist mithin nur eine von vielen Rechtsquellen zur Regelung des Datenschutzes in Deutschland. Nichts desto trotz wird diese Arbeit vertieft nur auf die Regelungen des BDSG eingehen, ist es doch Basis und Vorbild für die sonstigen datenschutzrechtlichen Regelungen. Zudem werden sich die in dieser Arbeit hervorgehobenen RFID-Anwendungen im Bereich der Privatwirtschaft mangels einschlägiger spezialgesetzlicher Regelungen an den Vorgaben des BDSG messen lassen müssen.

a) Allgemeines

aa) Gesetzgebungskompetenzen

Datenschutz als solcher ist eine Materie, die keine eigenständige Gesetzgebungskompetenzregelung im Grundgesetz erfahren hat. Vielmehr sind Aspekte des Datenschutzes bei der Materie mit zu regeln, bei der sie auftreten. Aus dieser Überlegung ergibt sich auch, dass in vielen

[459] *Di Fabio* in: Maunz/Dürig, GG Art. 2 Rn. 135.

[460] Vgl. zur Rangordnung der einzelnen Gesetze das Schaubild bei *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 169.

Spezialgesetzen datenschutzrechtliche Vorschriften zu finden sind. Die Schaffung der entsprechenden Regeln richtet sich hierbei nach der Kompetenz des Bundes- bzw. Landesgesetzgebers für die zu Grunde liegende Regelungsmaterie. Neben den bereits erwähnten Gesetzen – TMG und TKG, RStV, Pressegesetze und Polizeigesetze der Länder – findet sich eine Reihe weiterer datenschutzrechtlich relevanter Gesetze.[461]

Für die Schaffung des BDSG musste in Ermangelung einer universalen Gesetzgebungskompetenz auf verschiedene Kompetenzregeln zurückgegriffen werden. Die Regelungskompetenz für Datenverarbeitungen der öffentlichen Stellen ergibt sich nach der Gesetzesbegründung aus der Annexkompetenz des Verwaltungsverfahrens zu den jeweiligen Sachkompetenzen der Art. 73 bis 75 GG.[462] Für Datenverarbeitung i.R.d. Verwaltungstätigkeiten des Bundes (Art. 74 ff. GG) war der Bundesgesetzgeber damit unproblematisch zuständig und für solche der Länder jedenfalls, soweit diese Bundesrecht ausführen, vgl. Art. 84 Abs. 1 S. 5, Abs. 2 GG (dies ist beispielsweise der Fall im Pass- und Ausweiswesen, für das der Bund die ausschließliche Gesetzgebungskompetenz inne hat, Art. 73 Abs. 1 Nr. 3 GG). Im Bereich der Datenverarbeitung im nicht-öffentlichen Bereich stützt der Bund seine Gesetzgebungskompetenz insbesondere auf Art. 74 Nr. 1, 11 und 12 GG, weil eine einheitliche Regelung des Datenschutzes zur Wahrung der Rechts- und Wirtschaftseinheit erforderlich ist.[463]

Für den Landesgesetzgeber bleibt damit nur ein schmaler Bereich nämlich insbesondere der der Regelung solcher Verfahrensvorschriften, bei denen die Länder entweder Landesrecht oder Bundesrecht als eigene Angelegenheiten ausführen und im letzteren Falle nur, soweit der Bundesgesetzgeber keine einheitlichen Verwaltungsvorschriften erlässt, Art. 70, 83, 84 Abs. 1 und 2 GG. Ansonsten liegt die Regelung der datenschutzrechtlich wichtigen Materie des Polizei- und Ordnungswesens bei den Ländern. Entsprechend regeln die Polizeigesetze der Länder auch den Datenschutz bei polizei- und ordnungsrechtlichen Maßnahmen wie z.B. der präventiven TK-Überwachung, vgl. § 15a i.V.m § 20 HSOG. Der Umgang mit im Rahmen der Veranstaltung von Rundfunk oder der Pressearbeit anfallenden personenbezogenen Daten ist wegen der entsprechenden Länderzuständigkeiten bei den einschlägigen Gesetzen mit geregelt worden.

bb) Entwicklung des Datenschutzrechts und BDSG

Das erste BDSG[464] trat bereits am 1.1.1979 in Kraft.[465] Dennoch war es nicht das erste Datenschutzgesetz in Deutschland – Hessen verabschiedete bereits 1970 ein erstes Datenschutzge-

---

[461] S. Auflistung bei *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 159 ff.

[462] Vgl. die Gesetzesbegründung zum BDSG 2001, das in Umsetzung der DSRL erlassen wurde: Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, BTDrucks 14/4329 vom 13.10.2000, abrufbar unter http://dipbt.bundestag.de/doc/btd/14/043/1404329.pdf (04.04.2013), S. 27.; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 160.

[463] Taeger/Gabel/*Taeger/Schmidt*, Einführung, Rn. 5.

[464] Vgl. zur Entwicklung *Büllesbach*, RDV 2002, 55, 56

[465] BGBl. I S. 201 vom 01.02.1977.

setz[466], das gleichfalls auch das erste Datenschutzgesetz weltweit war[467]. Seit dem wurde das BDSG 18 mal geändert. Wesentlich waren die Änderungen nach dem Volkszählungsurteil des BVerfG[468] (BDSG 90[469]) zur Umsetzung der vom BVerfG aufgestellten Anforderungen an Datenverarbeitungsmaßnahmen und im Rahmen der Umsetzung der DSRL (BDSG 01[470]).[471]

Bedenkt man die rasante Entwicklung im Bereich Technik und Internet, so erstaunt es, dass es nicht zwischenzeitlich zu weiteren, grundlegenden Änderungen des BDSG oder aber der Schaffung neuer, spezieller Datenschutzgesetze gekommen ist. Bestrebungen gibt es indes diverse. Eine der aktuelleren ist die in Planung befindliche Schaffung eines umfassenden Arbeitnehmerdatenschutzes. Nach dem entsprechenden Regierungsentwurf[472], der zurzeit in Bundestag und Bundesrat beraten wird, soll eine ganze Bandbreite neuer Regelungen als neuer Unterabschnitt mit der Überschrift „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ in den dritten Abschnitt über die Datenverarbeitung nicht-öffentlicher Stellen in das BDSG eingefügt werden.

Ein weiterer Vorstoß ist die Vorlage eines Gesetzentwurfs des Bundesministeriums des Innern zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht[473], demzufolge die Speicherung personenbezogener Daten in Telemedien im Internet unter besonders hohe Anforderungen gestellt werden soll, soweit hierdurch ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen herbeigeführt wird. Auch diese Regelung könnte in den

---

[466] GVBl. I 1970 S. 625.

[467] *Gola/Schomerus*, BDSG, Einleitung, Rn. 1.

[468] BVerfGE 65, 1 – Volkszählung.

[469] Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, BGBl. I S. 2954 vom 20.12.1990, in Kraft getreten am 01.06.1991.

[470] Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, BGBl. I S. 904 vom 18.05.2001, in Kraft getreten am 23.05.2001.

[471] Vgl. zu den Details des Entwicklungsprozesses, *Abel* in: Roßnagel, HdB DSR, 2.7 Geschichte des Datenschutzrechts, Rn. 38 ff.

[472] Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15. 12. 2010, BTDrucks 17/4230, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf (04.04.2013).

[473] Bundesministerium des Innern, Gesetzentwurf zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht vom 01.12.2010, abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile (04.04.2013), der die Einfügung folgender Regelung als neuen § 38b in das BDSG vorschlägt:

> § 38b Unzulässige Veröffentlichungen in Telemedien
>
> Die Veröffentlichung von personenbezogenen Daten in Telemedien durch Stellen im Sinne des § 1 Absatz 2, wodurch ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen herbeigeführt wird, ist unzulässig, soweit nicht eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene ausdrücklich und gesondert eingewilligt hat oder ein überwiegendes schutzwürdiges Interesse an der Veröffentlichung besteht. Ein besonders schwerer Eingriff in das Persönlichkeitsrecht des Betroffenen liegt insbesondere vor, wenn in Telemedien personenbezogene Daten veröffentlicht werden,
>
> 1. die geschäftsmäßig gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuspeicherung weiterer Daten ausgewertet wurden und die dadurch ein umfangreiches Persönlichkeits- oder Bewegungsprofil des Betroffenen ergeben können oder
>
> 2. die den Betroffenen in ehrverletzender Weise beschreiben oder abbilden.

Abschnitt über die Datenverarbeitungen nicht-öffentlicher Stellen im BDSG eingefügt werden.

Im Zuge der Debatte um Googles Straßenansichtsdienst „Street View“ haben Vertreter der entsprechenden Branche gemeinsam mit dem BITKOM-Verband einen Datenschutz-Kodex für Geodatendienste[474] vorgestellt. Der Kodex sieht insbesondere Regeln zum Widerspruch Betroffener und Transparenzvorschriften für die Unternehmen vor. Zwar hat dieser Kodex nicht den Rang eines Gesetzes und kann entsprechend nicht von den offiziellen Datenschutzbehörden mittels Sanktionen durchgesetzt werden. Allerdings sieht der Kodex eine Einrichtung für freiwillige Selbstkontrolle vor, die gegen Verstöße der Kodex-Unterzeichner vorgehen kann. Solche Selbstverpflichtungen werden vom BDSG ausdrücklich in § 38a gefördert.[475] Abschließend verbindlich sind sie indes nicht.

Weiterhin wurde das Telekommunikationsgesetz (TKG) im Rahmen der Umsetzung des EU Telekom Pakets von 2009[476] geändert. Durch das verabschiedete Gesetz[477] wurden umfassende Änderungen im TKG vorgenommen, so auch im Bereich des Datenschutzes im Telekommunikationsbereich. U.a. ist eine allgemeine Benachrichtigungspflicht für Verstöße gegen datenschutzrechtliche Vorschriften implementiert werden (neuer § 109a TKG). Eine weitere Regelung ist indes für die vorliegende Arbeit besonders interessant. Der Europäische Gesetzgeber hat – wie bereits oben angesprochen – in Richtlinie 2009/136/EG die Änderung der eDSRL dahingehend vorgenommen, dass der Anwendungsbereich auf „öffentliche Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen“ ausgedehnt wird. Durch die TKG-Novelle wurde § 91 entsprechend angepasst:

> § 91 TKG Anwendungsbereich
>
> (1) Dieser Abschnitt regelt den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, **die Datenerfassungs- und Identifizierungsgeräte unterstützen** [Hervorhebung eingef. d. Verf.], erbringen oder an deren Erbringung mitwirken. (…)

---

[474] BITKOM, Datenschutz-Kodex für Geodatendienste, Stand Dezember 2010, abrufbar unter http://www.bitkom.org/files/documents/Datenschutz_Kodex.pdf (04.04.2013).

[475] S. hierzu unten E.II.3.a)aa).

[476] Das EU Telekom Paket besteht maßgeblich aus den zwei Richtlinien: Richtlinie 2009/136/EG (oben Fn. 382) und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz) und Richtlinie 2009/140/EG (des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und –dienste), ABl. L 337 vom 18.12.2009, S. 11-69, abrufbar unter http://eur-lex.europa.eu/JOIndex.do?year=2009&serie=L&textfield2=337&Submit=Suche&_submit=Suche&ihmlang=de (04.04.2013).

[477] Gesetz vom 03.05.2012 – BGBl I 2012 Nr. 19 vom 09.05.2012, S. 958, Berichtigung vom 08.08.2012 – BGBl I 2012 Nr. 37 vom 20.08.2012, S. 1717.

Unter den Begriff solcher Datenerfassungs- und Identifizierungsgeräte sollen nach der Gesetzesbegründung, die sich stark an dem entsprechenden Erwägungsgrund in der europäischen Änderungsrichtlinie 2009/136/EG orientiert, RFID-Anwendungen fallen.[478]

Diese Neuregelung ist allerdings nicht über zu bewerten. Zwar ist es ein Zeichen von Transparenz, dass der Gesetzgeber – wenn auch nur auf Drängen aus Brüssel – die Einbeziehung von RFID-Anwendungen in den Anwendungsbereich des TKG-Datenschutzes aufnehmen wird. Bei genauer Betrachtung zeigt sich indes, dass dies auch ohne eine solche Klarstellung der Fall ist, sofern das TKG überhaupt anwendbar ist. Der TKG-Datenschutz regelt schließlich den Schutz personenbezogener Daten beim Telekommunikationsvorgang in öffentlichen Kommunikationsnetzen. Sofern eine RFID-Anwendung also an ein öffentliches Kommunikationsnetz angeschlossen ist, unterfällt sie bei Vorliegen der weiteren Anwendungsvoraussetzungen (hierzu sogleich) auch nach jetziger Gesetzeslage dem Grundsatz nach dem TKG-Datenschutz im dort geregelten Umfang.

cc) Verhältnis zu spezialgesetzlichen bundesrechtlichen Normen: TKG und TMG

Das BDSG ist im Verhältnis zu anderen Gesetzen, die datenschutzrechtliche Regelungen enthalten, *lex generalis* und damit nur nachrangig anzuwenden. Das ergibt sich bereits aus dem in § 1 Abs. 3 BDSG geregelten Subsidiaritätsgrundsatz. Der Subsidiaritätsgrundsatz gilt aber nur insoweit, wie das *lex specialis* Regelungen trifft. Bei einem Blick in TKG und TMG wird dies deutlich: Beide Gesetze regeln jeweils nur den Umgang mit ganz bestimmten personenbezogenen Daten, nämlich Bestands- und Verkehrsdaten bzw. Bestands- und Nutzungsdaten. Die Verarbeitung von Inhaltsdaten wird nicht geregelt. Sofern solche Inhaltsdaten erhoben und anderweitig verarbeitet werden sollen, müssen andere Rechtsvorschriften dies erlauben bzw. eine Einwilligung des Betroffenen vorliegen, vgl. § 4 Abs. 1 BDSG. Bei der inhaltlichen Überwachung von Telefonaten oder Datentransfers über das Internet zu Strafverfolgungszwecken sind beispielsweise die Vorschriften der StPO über die Telekommunikationsüberwachung zu berücksichtigen. Bei Fehlen einer spezialgesetzlichen Norm ist die Erhebung und Verarbeitung von Inhaltsdaten an den Vorschriften des BDSG zu messen.[479]

Infolge der oben genannten Änderung des TKG werden bei Erhebung von Bestands- und Verkehrsdaten im Zusammenhang mit RFID-Anwendungen die Regelungen zum Datenschutz im TKG denen des BDSG vorgehen. Indes ist zu berücksichtigen, dass dies nur die Kategorien der Bestands- und Verkehrsdaten, nicht die der Inhaltsdaten betrifft. Bestandsdaten sind nach der Definition in § 3 Nr. 3 TKG „Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“. Bestandsdaten sind damit die Daten, die erforderlich sind, damit der Telekommunikationsdiensteanbieter seine Rechte und Pflichten aus dem Vertragsverhältnis wahrnehmen und eine reibungslose Abwicklung des Vertrages von der

[478] Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen vom 02.03.2011, BRDrucks 129/11 (TKG-E Regierungsentwurf), abrufbar unter http://dipbt.bundestag.de/dip21/brd/2011/0129-11.pdf (04.04.2013), S. 138.

[479] *Roßnagel* in: Roßnagel, HdB DSR, 7.9 Datenschutz in Tele- und Mediendiensten, Rn. 59.

Erbringung der Leistung bis hin zu ihrer Bezahlung gewährleisten kann. Solche Daten sind insbesondere Anrede, Name, Vorname, Anschrift, Anschlussnummer, Geburtsdatum, technische Daten des Anschlusses, die Art der Endeinrichtung, rechnungsrelevante Daten wie Bankverbindungen oder Einzugsermächtigungen u.ä.[480] Verkehrsdaten sind gem. § 3 Nr. 30 TKG „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden", also insbesondere Zeit und Dauer der Verbindung. § 95 TKG präzisiert, welche Verkehrsdaten unter welchen Voraussetzungen erhoben und verarbeitet werden dürfen. Dies sind insbesondere Nummern und Kennungen, Beginn, Ende und Dauer der Verbindung sowie der in Anspruch genommene Telekommunikationsdienst. Die auf einem RFID-Tag gespeicherten Daten erfüllen diese Kriterien nicht. Sie beziehen sich nicht auf den Telekommunikationsvorgang. Vielmehr sollen mittels Telekommunikationsvorgang die auf dem RFID-Tag gespeicherten Daten übermittelt werden. Damit sind sie vergleichbar mit dem gesprochenen Wort bei einem Telefonat oder dem geschrieben Wort bei einer E-Mail. Sie sind damit als Inhaltsdaten zu qualifizieren.[481] Folglich unterfallen sie – die sonstigen Anwendungsvoraussetzungen außen vor gelassen – nicht den Regelungen des TKG. Zudem richten sich die datenschutzrechtlichen Vorschriften aus dem TKG an den Anbieter öffentlich zugänglicher Telekommunikationsdienste, § 91 Abs. 1 TKG. Die für die Verarbeitung der RFID-Daten verantwortlichen Stellen dürften diese Voraussetzung in den wenigsten Fällen erfüllen. Vielmehr werden die Betreiber von RFID-Systemen regelmäßig auf einen dritten Internetzugangsprovider zurückgreifen, um die anfallenden Daten andernorts zu transferieren (vgl. hierzu bereits oben D.I.2.b). Nicht der RFID-Systembetreiber ist damit Adressat der Regelungen des TKG sondern der Internetzugangsprovider als Telekommunikationsanbieter.

Ähnlich sieht es bei den Datenschutzvorschriften im TMG aus. Die Definition über Bestandsdaten in § 14 Abs. 1 S. 1 TMG korreliert mit der im TKG. Nutzungsdaten sind gem. § 15 Abs. 1 S. 1 TMG solche Daten, die erforderlich sind, „um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen". § 15 Abs. 1 S. 2 TMG konkretisiert dies dahingehend, dass insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien unter den Begriff der Nutzungsdaten fallen. Hierzu gehören auch technische Steuerungsinformationen, wie insbesondere die IP-Adresse des Nutzers oder Cookies.[482] Auf einem RFID-Tag gespeicherten Daten sind hingegen jedenfalls nach jetzigem Technikstand nicht als solche Nutzungsdaten zu qualifizieren. Jedenfalls zum jetzigen Zeitpunkt ist nicht ersichtlich, inwiefern RFID-Tag-Daten bei der Erbringung von Telemediendiensten anfallen könnten, wie dies beispielsweise bei der IP-Adresse eindeutig der Fall ist. Für die Zukunft sind entsprechende Szenarien allerdings nicht ausgeschlossen. Zudem richten sich die datenschutzrechtlichen Vorschriften aus dem TMG wiederum nur an die Anbieter von Telemediendiensten und damit grundsätzlich nicht an die Betreiber von RFID-Anwendungen.

---

[480] Taeger/Gabel/*Munz*, § 95 TKG Rn. 6.

[481] Zum Begriff der Inhaltsdaten Taeger/Gabel/*Zscherpe*, § 14 TMG, Rn. 19 ff..

[482] Taeger/Gabel/*Munz*, § 15 TMG Rn. 18.

Damit wird es zunächst bei der Anwendung des BDSG im Rahmen der *Leading Scenarios* bleiben.

dd) Gesetzesstruktur

Das BDSG gliedert sich grob in sechs Abschnitte.[483] Im Unterschied zur DSRL, die es umsetzt, differenziert es zwischen Datenverarbeitungsmaßnahmen öffentlicher und nicht-öffentlicher Stellen, wie sich bereits im ersten Abschnitt in § 2 zeigt. Weiterhin finden sich im ersten Abschnitt allgemeine und gemeinsame Bestimmungen. Hierzu gehören u.a. die weiteren Begriffsbestimmungen (§ 3), der Grundsatz des präventiven Verbots mit Erlaubnisvorbehalt (§ 4) sowie der Datenvermeidung und Datensparsamkeit (§ 3a), die Regelung zur Einwilligung (§ 4a), die Regelung zur Übermittlung personenbezogener Daten ins Ausland sowie an über- und zwischenstaatliche Stellen (§ 4b), die Vorschriften zur Meldepflicht und zum behördlichen bzw. betrieblichen Datenschutzbeauftragten (§§ 4d ff.), die Regelung zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien (§ 6c) sowie den anzuwendenden technischen und organisatorischen Maßnahmen (§ 9 mit Anlage). Im zweiten Abschnitt ist die Datenverarbeitung der öffentlichen Stellen geregelt. Hierzu gehören die Rechtmäßigkeitsvoraussetzungen der Verarbeitung (§§ 13 bis 16), die Rechte des Betroffenen (§§ 19 bis 21) sowie die Regelungen über den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (§§ 22 bis 26). Der dritte Abschnitt regelt die Datenverarbeitung der nicht-öffentlichen Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen. Auch hier findet sich die Untergliederung in Rechtmäßigkeitsvoraussetzungen (§§ 28 bis 32) und Betroffenenrechte (§§ 33 bis 35). Weiterhin finden sich Regelungen zu den Aufsichtsbehörden (§ 38) und zu Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen (§ 38a)[484]. In den Abschnitten vier bis sechs finden sich Sonder-, Schluss- und Übergangsvorschriften und in deren Anschluss die Anlage zu § 9 S. 1 über die von der datenverarbeitenden Stelle zu ergreifenden technischen und organisatorischen Maßnahmen.

Dieser Maßnahmenkatalog ist auf RFID-Anwendungen grundsätzlich anzuwenden. Im Folgenden soll untersucht werden, ob die vorhandenen Regelungen ausreichen, um den für das informationelle Selbstbestimmungsrecht drohenden Gefahren[485] wirksam zu begegnen.

b) Anwendungsvoraussetzungen

Der Anwendungsbereich des BDSG ist gem. § 1 Abs. 2 BDSG eröffnet, wenn personenbezogene Daten durch öffentliche Stellen oder nicht-öffentliche Stellen erhoben, verarbeitet oder genutzt werden.

aa) Personenbezogene Daten

Zentrales Merkmal ist wie auch bei der DSRL der Begriff der personenbezogenen Daten.

---

[483] Vgl. Schaubild bei *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 252.

[484] BITKOM-Datenschutzkodex zu Geodatendiensten, oben Fn. 474.

[485] Vgl. oben C.II.

> § 3 Weitere Begriffsbestimmungen
>
> (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
>
> (…)

Zwar weicht der Wortlaut dieser Definition geringfügig von der in der DSRL verwendeten ab. Ihre Auslegung folgt aber den gleichen Grundsätzen. Der deutsche Gesetzgeber war insoweit an die Vorgaben des europäischen Gesetzgebers gebunden; die in Art. 5 DSRL vorgesehene Ausgestaltungsfreiheit der nationalen Gesetzgeber bezieht sich lediglich auf die Rechtmäßigkeitsvoraussetzungen der Datenverarbeitungen, nicht hingegen die Begriffsbestimmungen. Insofern gilt hier zunächst bei dem Begriff der personenbezogenen Daten und der konkreten Anwendung auf die *Leading Scenarios* im Rahmen der DSRL gesagtes.[486]

bb) Erhebung, Verarbeitung oder Nutzung

Weiterhin müssen die Daten erhoben, verarbeitet oder genutzt werden. Während die DSRL *per definitionem* keinen Unterschied zwischen den verschiedenen Verarbeitungsstufen macht – in Art. 2 b) DSRL findet sich vielmehr eine Definition für die „Verarbeitung personenbezogener Daten", die auch das Erheben und alle nachfolgenden Verarbeitungsschritte umfasst – differenziert das BDSG. In § 3 Abs. 3 bis 5 BDSG finden sich Definitionen für das Erheben, sich anschließende Verarbeitungen und, für alle Verwendungen, die nicht Verarbeitung sind, die Nutzung. Im Ergebnis ergibt sich indes kein Unterschied zu den Anwendungsvoraussetzungen der DSRL, weil das BDSG insgesamt den gleichen Bereich abdeckt. Insofern wird auch für das BDSG im Folgenden der Begriff des Verarbeitens synonym für alle Stufen des Umgangs mit personenbezogenen Daten verwendet.

cc) Verantwortliche Stelle

Zuletzt müssen die Daten durch eine im BDSG genannte verantwortliche Stelle verarbeitet werden. Das BDSG findet grundsätzlich Anwendung bei allen Datenverarbeitungsmaßnahmen durch öffentliche oder nicht-öffentliche Stellen. Die öffentlichen Stellen umfassen gem. § 1 Abs. 2 Nr. 1 und 2 BDSG alle öffentlichen Stellen des Bundes und der Länder. Bei den öffentlichen Stellen der Länder gilt – aus kompetenzrechtlichen Gründen – zunächst der Vorbehalt etwaiger landesrechtlicher Regelungen und zudem die Einschränkung, dass Stellen der Länder nur betroffen sind, sofern sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt. Hinsichtlich der nicht-öffentlichen Stellen gilt die Ausnahme, dass die Datenverarbeitung ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten erfolgt, § 2 Abs. 2 Nr. 3 BDSG

[486] Oben D.I.2.a)aa)aaa).

dd) Leading Scenarios

Szenario 1

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis): Personenbezogene Daten sind unstreitig involviert;

In Szenario 1 sind wie oben festgestellt personenbezogene Daten betroffen. Die Erhebung erfolgt hierbei zunächst durch die Stelle, die das RFID-Tag mit den betreffenden Daten beschreibt und anschließend an den Betroffenen aushändigt. Im Fall des Personalausweises und Reisepasses sind dies die Meldebehörden, mithin öffentliche Stellen. Im Fall der ÖPNV-Tickets das entsprechende Beförderungsunternehmen, also regelmäßig nicht-öffentliche Stellen.

Die Daten können im weiteren Verlauf ihrer Lebensdauer aber auch durch andere Stellen erhoben werden. Zu denken ist hier bei den Ausweispapieren zunächst an Zollstellen oder aber Polizeibehörden im Rahmen der Identitätsfeststellung. Sofern die Daten unverschlüsselt oder nur unzureichend verschlüsselt auf dem Tag gespeichert sind, kann theoretisch jede Person mit einem kompatiblen Lesegerät die Daten auslesen und damit erheben (so z.B. auch Identitätsdiebe). Vor diesem Hintergrund ist jedenfalls bei den Ausweisdokumenten gesetzlich festgelegt worden, dass die RFID-Daten verschlüsselt werden müssen, vgl. § 4 Abs. 3 S. 2 PassG, § 5 Abs. 6 PAuswG. Soweit die Daten mittels wirksamer Verschlüsselung nicht oder jedenfalls nur verfremdet – also anonymisiert – ausgelesen werden können, entfällt die Anwendbarkeit des BDSG für solche Erhebungsvorgänge. Es fehlt in diesen Fällen bereits am Kriterium der personenbezogenen Daten.

Sich an die Erhebung anschließende Verarbeitungsschritte können von allen Stellen vorgenommen werden, die einmal im Besitz der Daten sind. Hierbei ist insbesondere an Speicherung aber auch an Übermittlung an Dritte zu denken. Hinsichtlich der Ausweisdokumente hat der Gesetzgeber die Verwendung der ausgelesenen Daten spezialgesetzlich stark reglementiert. So dürfen die autorisierten Stellen die auf dem RFID-Tag gespeicherten Daten in Pass und Personalausweis nur zum Zwecke der Feststellung der Echtheit des Ausweisdokuments oder der Identität des Ausweisinhabers auslesen. Im Anschluss sind die erhobenen Daten unverzüglich zu löschen, § 16a PassG, § 17 PAuswG, es darf also keine weitergehende Verarbeitung stattfinden. PassG und PAuswG fungieren als abschließende Sonderregelungen im Verhältnis zum BDSG.[487]

Für ÖPNV-Tickets oder ähnliche in der Privatwirtschaft eingesetzte RFID-Tags i.S.v. Szenario 1 gibt es solche speziellen Regeln nicht. Die Erhebung und Verarbeitung der entsprechenden Daten hat sich demnach nach den allgemeinen Vorschriften des BDSG zu richten.

[487] *Schulz* in: Schliesky, Gesetz über Personalausweise und den elektronischen Identitätsnachweis, § 14 Rn. 3, § 17 Rn. 2.

Szenario 2

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert;

Auch in Szenario 2 werden personenbezogene Daten verwendet. Die RFID-Tag ausgebende Stelle ist diejenige, die die Implantierung des Chips veranlasst. Mangels bekannter Anwendungen im öffentlichen Bereich – der Einsatz von RFID wie in einigen U.S. amerikanischen oder auch einem niederländischen Gefängnis[488] in Deutschland wäre indes ein solcher Fall – dürften sich Fälle der Implantierung von VeriChips o.ä. auf den Privatsektor beschränken. Die im Hintergrundsystem gespeicherten Daten werden von der Tag ausgebenden Stelle erhoben und gespeichert. Sie werden von dieser Stelle auch weiterverarbeitet, sofern dies Gegenstand der vertraglichen Beziehung ist. Dritte Stellen können regelmäßig nur auf die RFID-Tag-Nummer zugreifen. Diese wird regelmäßig nicht verschlüsselt gespeichert werden. Da aber wie oben festgestellt auch diese Identifizierungsnummer personenbezogenes Datum ist, findet bei jedem Auslesevorgang eine datenschutzrechtlich relevante Erhebung mit sich gegebenenfalls anschließenden weiteren Verarbeitungsschritten statt. Alle Erhebungs- und Verarbeitungsmaßnahmen gleich von welcher Stelle durchgeführt, müssen sich mangels spezialgesetzlicher Regelungen an den Regelungen des BDSG messen lassen.

Szenario 3

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte);

Für die im Rahmen von Szenario 3 im Hintergrundsystem gespeicherten Daten ergibt sich oben zu Szenario 2 gesagtes. Die auf dem Gegenstand – z.B. einer Kundenkarte – gespeicherte Identifikationsnummer ist nach den vorangegangenen Erläuterungen als personenbezogenes Datum zu qualifizieren. Auch diese Identifikationsnummern werden regelmäßig nicht verschlüsselt werden. Insofern können diese, genauso wie die auf einem VeriChip gespeicherte Identifikationsnummer, grundsätzlich von jedermann mit einem kompatiblen Lesegerät ausgelesen und damit erhoben werden. Das Anlegen von Bewegungs- und Verhaltensprofilen – also insbesondere das Zusammenführen einzelner Daten – stellte eine weitergehende Verarbeitungsmaßnahme dar.

Szenario 4

(4) EPC:

Auf dem RFID-Tag ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert, das RFID-Tag ist an einem Gegenstand angebracht, der von einem Menschen mitgeführt wird (alle Verkaufsprodukte, insbesondere solche, die längerfristig mitgeführt werden); im Hintergrundsystem sind nur weiterführende Daten zum Produkt gespeichert.

[488] Vgl. oben C.II.1.

Nach obigen Ausführungen stellen auch auf Produktebene eingesetzte Identifikationsnummern wie in Szenario 4 personenbezogene Daten dar, sofern die getaggten Gegenstände von Personen mitgeführt werden. Diese Daten werden von jeder Person erhoben, die die Daten ausliest. Dies muss nicht zwangsläufig nur die ausgebende Stelle – also der Einzelhändler, der die getaggten Gegenstände verkauft – sondern kann jede Stelle – und zwar sowohl öffentliche als auch nicht-öffentliche Stellen – sein, die eine kompatible RFID-Infrastruktur betreibt und alle RFID-Daten einliest, die in den Einzugsbereich eines ihrer Lesegeräte gelangen. Auch solche Verarbeitungsvorgänge haben sich mangels spezialgesetzlicher Regelung an die Vorgaben des BDSG zu halten.

c) Allgemeine Zulässigkeitsvoraussetzungen der Datenverarbeitung

Nach der Gesetzesstruktur sind zunächst bei jeder Datenverarbeitung, egal ob von öffentlichen oder nicht-öffentlichen Stellen durchgeführt, allgemeine Zulässigkeitsvoraussetzungen zu beachten. Diese sind in Ergänzung zum Vorliegen eines jeweiligen Erlaubnistatbestandes zu prüfen.

aa) Präventives Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG

Zentrale Norm des BDSG ist § 4 Abs. 1. Dieser regelt den Grundsatz, dass jede Datenerhebung und -verarbeitung nur zulässig ist, soweit eine gesetzliche Erlaubnis oder Anordnung vorliegt oder der Betroffene eingewilligt hat. Die gesetzliche Erlaubnis kann sich aus einer spezialgesetzlichen Norm ergeben oder aber aus dem BDSG selbst, welches als Auffanggesetz fungiert, vgl. § 1 Abs. 3 BDSG.

Wie bereits oben festgestellt, finden jedenfalls die datenschutzrechtlichen Regelungen und damit auch Erlaubnistatbestände aus TKG und TMG keine Anwendung auf RFID-Daten. Im Pass- und Ausweiswesen gilt hingegen die Erlaubnis der zuständigen Stelle zur Erhebung der auf dem RFID-Tag gespeicherten Daten nach den Vorschriften des Pass- bzw. Personalausweisgesetzes. Im PassG sind dies §§ 16a, 17 und 18, im PAuswG §§ 14 ff. Für die Erhebung von RFID-Daten im Einzelhandel oder sonstigen RFID-Anwendungen in der Privatwirtschaft gibt es keine spezialgesetzlichen Erlaubnistatbestände. Ihre Rechtmäßigkeit richtet sich demnach nach den Vorschriften des BDSG. Bei den Erlaubnistatbeständen wird unterschieden zwischen öffentlichen und nicht-öffentlichen Stellen. Diese werden unten gesondert dargestellt. Für alle Datenerhebungs- und -verarbeitungsmaßnahmen ergibt sich zudem die Möglichkeit der Legitimierung mittels Einwilligung des Betroffenen.

bb) Einwilligung, § 4a BDSG

Die Einwilligung in die Erhebung und Verarbeitung der eigenen personenbezogenen Daten gem. § 4a BDSG ist der wahrscheinlich deutlichste einfachgesetzliche Ausdruck des verfassungsrechtlich gewährleisteten Rechts auf informationelle Selbstbestimmung, ist sie doch Selbstbestimmung in ihrer konzentrierten Form. Dass dieser hehre, aus Zeiten des Einsatzes von Großrechnern und äußerst begrenzten Datensammelmöglichkeiten stammende Ansatz heute zunehmend nicht mehr erreicht sondern in vielen Fällen – bei Alternativlosigkeit zur

Datenhingabe – gar konterkariert wird[489], mag zutreffen. Eine solche Einschätzung ändert indes nichts daran, dass die Regelung Bestand hat und folglich in jedem datenschutzrechtlichen Szenario, das mittels Einwilligung seitens des Betroffenen gerechtfertigt sein soll, die Wirksamkeit eben dieser Einwilligung zu prüfen ist. Die Einwilligung, eine rechtsgeschäftliche Erklärung[490], muss hierbei sowohl bestimmten formellen als auch inhaltlichen Anforderungen genügen.

In formeller Hinsicht muss die Einwilligung zum richtigen Zeitpunkt – nämlich vor der Datenerhebung oder -verarbeitung – von einem einsichtsfähigen Betroffenen höchstpersönlich regelmäßig schriftlich abgegeben werden. Das Erfordernis der Abgabe der Einwilligung vor der Datenerhebung oder -verarbeitung führt dazu, dass auch bei einer nachträglichen zustimmenden Erklärung des Betroffenen, eine bereits erfolgte Datenverarbeitung rechtswidrig bleibt. Zwar kann eine bereits erfolgt Verarbeitung nicht mehr rückgängig gemacht werden, hier bleibt nur die Feststellung der Rechtswidrigkeit, aber lediglich erhobene Daten sind umgehend zu löschen, §§ 20 Abs. 2 Nr. 1, 35 Abs. 2 Nr. 1 BDSG, und jede weitergehende Verarbeitung ist zu unterlassen.

Das Schriftformerfordernis stellt die Regel dar, Ausnahmen können nur in eng begrenzten Fällen – gesetzlich geregelt ist z.B. der Fall der Datenverarbeitung zu Werbezwecken, § 28 Abs. 3 BDSG – durchgreifen, und zwar dann, wenn besondere Umstände es rechtfertigen, eine andere Form für die Einwilligungserklärung zu wählen. In keinem Fall darf ein Abrücken von der Schriftform zu einem kompletten Ausbleiben der Einwilligung führen. Faktisch kann die schriftliche Einwilligung daher bei Vorliegen besonderer Umstände – wie z.B. Notfallsituationen mit entsprechendem Zeitdruck – durch eine mündliche ersetzt werden. Unter keinen Umständen genügt eine konkludente, stillschweigende oder gar mutmaßliche Einwilligung.[491]

In inhaltlicher Hinsicht muss die Erklärung des Betroffenen freiwillig, informiert und bestimmt erfolgen. Freiwilligkeit – in Umsetzung der Vorgabe aus Art. 2 h) DSRL, dass die Einwilligung „ohne Zwang“ erfolgen muss – bedeutet, dass eine Erklärung des Betroffenen unter Zwang und zwar auch faktischem Zwang unwirksam ist. An dieses Kriterium lehnt sich die Frage über die Brauchbarkeit des Instituts der Einwilligung als solcher an: Wenn ein Geschäft nicht abgeschlossen, oder ein Dienst nicht in Anspruch genommen werden kann – und zwar nicht tatsächlich, sondern weil die Gegenseite auf die Erteilung der Einwilligung zur Erhebung bestimmter personenbezogener Daten besteht – dann befindet sich der Betroffene in einer derartigen faktischen Zwangslage, dass ihm gar nichts anderes übrig bleibt, als diese Einwilligung zu erteilen. Infolge des Kopplungsverbots ist es deshalb datenverarbeitenden Stellen untersagt, die Erreichung eines (Geschäfts-)Zwecks von der Erteilung der Einwilli-

[489] So z.B. *Simitis* in: Simits, BDSG, § 4a Rn. 3 ff; *Däubler* in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 4a Rn. 1.

[490] *Simitis* in: Simits, BDSG, § 4a Rn. 20.

[491] *Simitis* in: Simits, BDSG, § 4a Rn. 43, 44.

gung in die Erhebung mit dem Zweck nicht im Zusammenhang stehender Daten abhängig zu machen.[492]

cc) Direkterhebungsgrundsatz, § 4 Abs. 2 BDSG

Ein weiterer wesentlicher Grundsatz im BDSG ist der sich aus § 4 Abs. 2 BDSG ergebende Direkterhebungsgrundsatz. Nach diesem Grundsatz sind personenbezogene Daten beim Betroffenen zu erheben. Nur in eng umrissenen Ausnahmefällen darf die Erhebung ohne die Mitwirkung und damit vor allem ohne seine Kenntnis[493] vorgenommen werden und dann auch nur, soweit keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürde Interessen des Betroffenen beeinträchtigt werden. Als erste Ausnahme sieht das Gesetz vor, dass eine Rechtsvorschrift die Erhebung vorsieht oder zwingend voraussetzt. Weiterhin ist die Erhebung ohne Mitwirkung des Betroffenen möglich, soweit die zu erfüllende Verwaltungsaufgabe – für öffentliche Stellen – oder der zu erfüllende Geschäftszweck – für nicht-öffentliche Stellen – dies erforderlich macht.[494] Zuletzt kann eine Erhebung bei Dritten erfolgen, soweit die Erhebung beim Betroffenen selbst einen unverhältnismäßig großen Aufwand erfordern würde.

Der Grundsatz des Mitwirkungserfordernisses beim Betroffenen setzt den Selbstbestimmungsgedanken des Datenschutzrechts um. Hintergrund ist, dass nur ein informierter Betroffener, der weiß, wer wann und bei welcher Gelegenheit welche Daten über ihn erhebt und verarbeitet[495], effektiv von seinen Rechten auf Auskunft, Berichtigung und Löschung Gebrauch machen kann.[496] Entsprechend hat der Gesetzgeber als Ergänzung eine Informationspflicht für die datenverarbeitende Stelle für die Fälle geschaffen, in denen der Betroffene nicht bereits auf andere Weise Kenntnis über die wesentlichen Punkte der Datenerhebung- und Verarbeitung erlangt hat, § 4 Abs. 3 BDSG. Die Information des Betroffenen muss hierbei vor der Datenerhebung stattfinden, denn nur dann kann der Betroffene eine bewusste Entscheidung fällen.[497]

Die Mitwirkung des Betroffenen kann sowohl in aktiver als auch in passiver Weise erfolgen. Die aktive Mitwirkung ist z.B. das Antworten auf eine Frage zur eigenen Person oder das Ausfüllen eines Datenblatts. Eine passive Mitwirkung setzt die ausdrückliche und bewusste – also informierte – Duldung der Datenerhebung voraus und funktioniert nur, soweit dem Betroffenen eine tatsächliche Möglichkeit zur Entziehung verbleibt.[498] Alles andere widerspräche dem Grundgedanken der Selbstbestimmung.

---

[492] Taeger/Gabel/*Taeger*, § 4a BDSG, Rn. 54.

[493] Taeger/Gabel/*Taeger*, § 4 BDSG, Rn. 56.

[494] *Sokol* in: Simitis, BDSG, § 4 Rn. 32, 34.

[495] BVerfGE 65, 1 (43) – Volkszählung.

[496] Taeger/Gabel/*Taeger*, § 4 BDSG, Rn. 56; *Sokol* in: Simitis, BDSG, § 4, Rn. 23.

[497] *Gola/Schomerus*, BDSG, § 4 Rn. 29.

[498] *Sokol* in: Simitis, BDSG, § 4, Rn. 23.

Sofern zwar die Erhebung der Daten beim Betroffenen erfolgt aber ohne seine Kenntnis, ist der Direkterhebungsgrundsatz verletzt. Eine solche Erhebung ist nur bei Vorliegen einer Ausnahme rechtmäßig.

dd) Datenübermittlung ins Ausland, §§ 4b und 4c BDSG

Die Übermittlung personenbezogener Daten ins Ausland wird in Umsetzung der DSRL auch vom BDSG zusätzlich zu den allgemeinen Rechtmäßigkeitsvoraussetzungen für Datenverarbeitungen unter besondere Voraussetzungen gestellt. Eine Welt mit ubiquitären RFID-Anwendungen, dezentralisierter Datenverarbeitung und umfassender Vernetzung einzelner Akteure wird ohne stetige Datenübermittlung nicht funktionieren. Die meisten der erhobenen Daten werden höchstwahrscheinlich in der „Cloud" gespeichert und zum Abruf durch den Berechtigten bereitgehalten werden. Vor diesem Hintergrund wird zunehmend das Augenmerk bei der Ausgestaltung von RFID-Anwendungen und -Infrastrukturen auf die Beachtung der Regeln zum internationalen Datentransfer zu richten sein.

Grob ist zwischen zwei Fällen der Datenübermittlung zu unterscheiden: Einerseits der Übermittlung an Stellen in einem anderen EU bzw. EWG-Staat sowie an die Organe und Einrichtungen der EU, § 4b Abs. 1 BDSG, und andererseits an Stellen außerhalb des beschriebenen Raums, sog. Drittstaaten, § 4b Abs. 2 und 3 BDSG. Vor dem Hintergrund eines harmonisierten Datenschutzrechts auf EU-Ebene sieht § 4b Abs. 1 BDSG entsprechend die Anwendung der Vorschriften über die Übermittlung innerhalb Deutschlands auch für die Fälle der ersten Kategorie vor, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des EU-Rechts fallen. Übermittlungen der ersten Kategorie sind damit quasi nur eine Variation der Weitergabe an inländische Stellen.[499]

Für Datentransfers der zweiten Kategorie, also Datenübermittlungen in Drittstaaten sowie solche, die nicht im Rahmen von Tätigkeiten erfolgen, die ganz oder teilweise in den Anwendungsbereich des EU-Rechts fallen, sieht § 4b Abs. 2 BDSG eine entsprechende Anwendung von Abs. 1 mit der Zugabe vor, dass bei überwiegendem schutzwürdigem Interesse des Betroffenen an dem Ausschluss der Übermittlung selbige unterbleiben muss. Das bedeutet, dass sich jede Datenübermittlung ins Ausland zunächst an den allgemeinen Rechtmäßigkeitsvoraussetzungen des BDSG messen lassen und im Falle einer Übermittlung nach Kategorie 2 zusätzlich die Abwägung mit etwaigen schutzwürdigen Interessen des Betroffenen vorgenommen werden muss. Dies gilt auch in Fällen des Datentransfers innerhalb eines Konzerns über Ländergrenzen hinweg.[500] Eine Übermittlung in ein Drittland ist indes nicht bei Veröffentlichung personenbezogener Daten auf einer Internetseite gegeben, soweit der Host-Provider ebenfalls seinen Sitz innerhalb der EU/EWG hat, unabhängig davon, dass die Website mittels Internetzugang von jedem Ort auf der Welt aus abrufbar ist.[501]

---

[499] *Simitis* in: Simitis, BDSG, § 4b Rn. 26.

[500] Taeger/Gabel/*Gabel*, § 4b BDSG Rn. 15.

[501] EuGH Urteil vom 6.11.2003 – Rs. C-101/01 (Bodil Lindqvist) oben Fn. 297, Rn. 71.

Ein überwiegendes schutzwürdiges Interesse des Betroffenen wird nach § 4b Abs. 2 S. 1 BDSG insbesondere dann angenommen, wenn die empfangende Stelle ein angemessenes Datenschutzniveau nicht gewährleistet. Ein überwiegendes Interesse des Betroffenen kann sich demnach aber auch aus anderen Gründen ergeben. Ob die empfangende Stelle ein angemessenes Datenschutzniveau gewährleistet, ist im Einzelfall und unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenübermittlung von Bedeutung sind, § 4b Abs. 3 BDSG.[502] Lediglich in eng umrissenen Ausnahmen, darf eine Übermittlung auch dann erfolgen, wenn die empfangende Stelle das erforderliche angemessene Schutzniveau nicht erreicht, § 4c Abs. 1 BDSG. Zu den Ausnahmen gehören u.a. die Einwilligung des Betroffenen, die Erforderlichkeit für die Abwicklung von Verträgen des Betroffenen mit der verantwortlichen Stelle oder aber von Verträgen im Interesse des Betroffenen zwischen der verantwortlichen Stelle und einem Dritten. Weiterhin besteht die Möglichkeit, dass die zuständige Aufsichtsbehörde bestimmte Übermittlungen genehmigt. Dies kann dann geschehen, wenn die verantwortliche – also die übermittelnde – Stelle ausreichende Garantien zum Schutz des Persönlichkeitsrechts des Betroffenen vorweist, insbesondere können diese sich ergeben aus Vertragsklauseln[503] – also Verträge zwischen der übermittelnden und der empfangenden Stelle – oder verbindlichen Unternehmensregeln (sog. *Binding Corporate Rules*) – bei konzerninternen Datenübermittlungen.

Problematisch ist regelmäßig die Beantwortung der Frage, wann ein angemessenes Datenschutzniveau bei der empfangenden Stelle gegeben ist. Die vom Gesetzgeber beispielhaft in § 4b Abs. 3 BDSG vorgesehenen Bewertungskriterien sind hierbei in einer Gesamtschau heranzuziehen. Im Ergebnis muss das Datenschutzniveau beim Empfänger dem über das BDSG geltenden Datenschutzniveau in Deutschland, jedenfalls im Hinblick auf die konkrete Datenverarbeitungsmaßnahme, wohl gleichwertig sein.[504] Gemäß ihrem Auftrag aus Art. 30 Abs. 1 b) DSRL hat die Artikel-29-Datenschutzgruppe im Laufe der Zeit eine Vielzahl Länder auf die Angemessenheit des bei ihnen herrschenden Datenschutzniveaus geprüft. Die betreffenden Entscheidungen wurden jeweils von der Kommission in Ausübung ihrer Kompetenz gem. Art. 25 Abs. 6 DSRL übernommen.[505] Bei den anerkannten Ländern ist eine Einzelfallbetrachtung der jeweiligen empfangenden Stelle zur Feststellung des angemessenen Datenschutzniveaus entbehrlich.[506] Für Datenübermittlungen in die USA gelten besondere Regeln.

---

[502] *Simitis* in: Simitis, BDSG, § 4b Rn. 48 ff.

[503] Die von der Kommission im Rahmen ihrer Kompetenz gem. Art. 26 Abs. 4 DSRL erlassenen Standartvertragsklauseln sind abrufbar unter http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (04.04.2013).

[504] Vgl. zum Streit *Simitis* in: Simitis, BDSG, § 4b Rn. 52, der Gleichwertigkeit fordert, und a.A. *Gola/Schomerus*, BDSG, § 4b Rn. 12, nach deren Ansicht es ausreicht, wenn dem Betroffenen beim Empfänger in Bezug auf die Verarbeitung ein Schutz zuteil wird, der dem Kernbestand der Schutzprinzipien der DSRL im Wesentlichen gerecht wird.

[505] Vgl. die Liste der Länder mit anerkanntem angemessenem Datenschutzniveau auf der Homepage der Kommission unter http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (04.04.2013).

[506] Taeger/Gabel/*Gabel*, § 4b BDSG Rn. 22.

Grundsätzlich besteht in den USA kein angemessenes Datenschutzniveau[507], sodass entsprechend Datenübermittlungen wegen der unwiderleglichen Vermutung aus § 4b Abs. 2 S. 2 BDSG dorthin eigentlich unterbleiben müssten. Um diesem Dilemma aus dem Weg zu gehen, hat die Kommission mit der US-Regierung die sog. *Safe-Harbor*-Grundsätze entwickelt und auf die Einhaltung dieser Grundsätze ihre Angemessenheitsentscheidung gestützt.[508] Nach der entsprechenden Entscheidung der Kommission gilt bei allen Unternehmen, die dem Safe-Harbor-Abkommen beitreten[509], dass sie das geforderte angemessene Datenschutzniveau gewährleisten und entsprechend Datentransfers an sie stattfinden dürfen.[510]

ee) Mobile personenbezogene Speicher- und Verarbeitungsmedien, § 6c BDSG

Der mit der BDSG-Reform von 2001 eingeführte § 6c BDSG könnte sich in Zukunft als besonders wichtig im Hinblick auf RFID-Anwendungen herausstellen. Die Norm stellt besondere Regeln für mobile personenbezogene Speicher- und Verarbeitungsmedien auf.

> § 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien
>
> (1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen
>
> 1. über ihre Identität und Anschrift,
>
> 2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
>
> 3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
>
> 4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen
>
> unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.
>
> (2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.
>
> (3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 6c BDSG statuiert Transparenz- und Informationspflichten für die verpflichtete Stelle, die zusätzlich zu den sonstigen Rechtmäßigkeitsvoraussetzungen für die jeweilige Datenverarbeitungsmaßnahme erfüllt werden müssen.

In § 3 Abs. 10 BDSG findet sich die dazugehörige Definition der betroffenen Medien:

> (10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,
>
> 1. die an den Betroffenen ausgegeben werden,
>
> 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

---

[507] Taeger/Gabel/*Gabel*, § 4b BDSG Rn. 23.

[508] Taeger/Gabel/*Gabel*, § 4b BDSG Rn. 23.

[509] Die gesamte Liste aller beigetretenen Unternehmen ist abrufbar unter http://safeharbor.export.gov/list.aspx (04.04.2013).

[510] Vgl. zur Kritik an den Regelungen im Safe-Harbor-Abkommen *Simitis* in: Simitis, BDSG, § 4b Rn. 73 ff.

> 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Auf den ersten Blick könnte man geneigt sein, RFID-Tags grundsätzlich dieser Definition und entsprechende Anwendungen damit den zusätzlichen Informationspflichten aus § 6c BDSG zu unterwerfen. Indes ist die Subsumtion problematisch. Insbesondere das Merkmal der automatisierten Verarbeitung in § 3 Abs. 10 Nr. 2 BDSG wird in der Literatur durchaus unterschiedlich interpretiert.[511] Dies hat maßgebliche Auswirkung auf die Anwendbarkeit in unterschiedlichen Anwendungen – so auch in RFID-Anwendungen.

Nach der Gesetzesbegründung fallen unter den Begriff der mobilen personenbezogenen Speicher- und Verarbeitungsmedien ausschließlich Medien, „auf denen personenbezogene Daten über die Speicherung hinaus automatisiert verarbeitet werden können (Nummer 2), die also mit einem Prozessorchip ausgestattet sind".[512] Dass neben der Speicherung auch eine weitergehende automatisierte Verarbeitung auf dem Medium möglich sein muss, ergibt sich wörtlich auch aus der Definition in § 3 Abs. 10 BDSG. Die Gesetzesbegründung geht nun davon aus, dass bloße Speichermedien wie z.B. CDs oder Magnetkarten nicht umfasst sind.[513] Die Literatur ist daraufhin teilweise davon ausgegangen, dass das bloße Auslesen der auf dem Medium gespeicherten Daten nicht ausreicht, um es als mobiles personenbezogenes Speicher- und Verarbeitungsmedium i.S.v. § 6c BDSG zu qualifizieren.[514] Verfehlt ist die Lesart, § 6c BDSG beziehe sich auf Speicher- *oder* Verarbeitungsmedien um hierüber zu einer Anwendung auch bei Medien zu kommen, auf denen Daten lediglich gespeichert sind.[515] Der Gesetzeswortlaut ist insoweit eindeutig, vgl. insbesondere § 3 Abs. 10 Nr. 2 BDSG, nach dem Daten auf dem betreffenden Medium gespeichert und *darüber hinaus* – also kumulativ und nicht alternativ – automatisiert verarbeitet werden können müssen.

Die Gesetzesbegründung äußert sich nicht abschließend dazu, ob tatsächlich ein bloßes Auslesen der auf dem Medium gespeicherten Daten kein über die Speicherung hinausgehender Verarbeitungsvorgang ist. Ginge man mit Teilen der o.g. Literaturmeinung eben hiervon aus, wären konsequent Medien wie die elektronische Gesundheitskarte, die neuen elektronischen Reisepässe und Personalausweise – und im Ergebnis somit auch die meisten sonstigen RFID-

---

[511] *Holznagel/Bonnekoh*, MMR 2006, 17 (21); *v. Westerhold/Döring*, CR 2004, 710 (714); *Hornung*, MMR 2006, XX (XXI); *Gola/Schomerus*, BDSG, § 6c Rn. 2; *Bizer* in: Simitis, BDSG, § 6c Rn. 15 ff.; *Scholz* in: Simitis, BDSG (2011), § 3 Rn. 272 ff.

[512] Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze (BDSG-ÄndG 2001) in der Fassung des Innenausschusses des Bundestages vom 04.04.2001, BTDrucks 14/5793, abrufbar unter http://dip21.bundestag.de/dip21/btd/14/057/1405793.pdf (04.04.2013), S. 60.

[513] BDSG-ÄndG 2001, oben Fn. 512, S. 60.

[514] *Holznagel/Bonnekoh*, MMR 2006, 17 (21); *v. Westerhold/Döring*, CR 2004, 710 (714); *Hornung*, MMR 2006, XX (XXI); *Gola/Schomerus*, BDSG, § 6c Rn. 2; *Bizer* in: Simitis, BDSG, § 6c Rn. 15 (für die elektronische Gesundheitskarte), 16 f. (für Signaturkarten), 18 ff. für elektronische Pässe und Personalausweise; im Ergebnis auch *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 105.

[515] So aber Taeger/Gabel/*Zscherpe*, § 6c BDSG Rn. 19.

Tags[516] – vom Anwendungsbereich des § 6c BDSG ausgeschlossen.[517] Für produktbezogene RFID-Tags soll dies nach allen Ansichten gelten. Orientiert man sich hingegen an den Vorgaben, die das BDSG selbst macht, kommt man – nach einer Auslegung anhand des Gesetzeswortlauts – zu einem anderen Ergebnis.

Der Begriff des Verarbeitens ist ausdrücklich in § 3 Abs. 4 BDSG definiert:

> (4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. (…)

Das Übermitteln unterfällt dem Begriff des Verarbeitens. Dieses ist wiederum in § 3 Abs. 4 Nr. 3 legal definiert:

> Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
>
> (…)
>
> 3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
>
> a) die Daten an den Dritten weitergegeben werden oder
>
> b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft, (…)

Die vom BDSG vorgesehene Verarbeitungsform des Übermittelns kann sowohl aktiv, § 3 Abs. 4 Nr. 3 a) BDSG, als auch passiv, § 3 Abs. 4 Nr. 3 b) BDSG erfolgen. Die passive Übermittlung ist das Einsehen oder *Abrufen* der betreffenden personenbezogenen Daten. Genau dieser Fall tritt bei mobilen Speichermedien ein, auf denen personenbezogene Daten gespeichert sind und die lediglich ausgelesen werden. Dem Wortlaut der einschlägigen Normen im BDSG nach ist gerade keine hierüber hinausgehende anderweitige Verarbeitung, wie etwa das Verändern der gespeicherten Daten mittels Prozessorchip erforderlich.[518]

Zusammenfassend: Im Falle mobiler personenbezogener Speicher- und Verarbeitungsmedien ist ein über die Speicherung hinausgehender Verarbeitungsvorgang erforderlich, dieser ist aber dem Gesetzeswortlaut nach – und entgegen der benannten Literaturmeinungen – bereits in einem etwaigen Auslese- sprich Übermittlungsvorgang zu sehen.

Zwar lässt die Gesetzesbegründung und der beispielhafte Ausschluss von CDs und Magnetkarten den Schluss darauf zu, dass der Gesetzgeber ein Mehr gegenüber dem „bloßen" Auslesen der Daten gesetzlich festschreiben wollte. Indes ist zu berücksichtigen, dass das Auslesen der genannten Medien jeweils einen physischen oder optischen Kontakt erfordert, der beim Auslesen von RFID-Tags gerade entbehrlich ist. Das Auslesen kann also unbemerkt vom Betroffenen stattfinden. In den benannten Beispielmedien der CD und Magnetkarte kann eine solche heimliche Auslesung nicht stattfinden. Und gerade um die Begrenzung der sich aus solchen unbemerkten Datenverarbeitungsmaßnahmen ergebenden Gefahren für das Persön-

[516] Komplexe RFID-Tags mit Rechenleistung und Sensortechnik, vgl. oben B.I.2.a), würden dennoch unter die Definition fallen.

[517] So jedenfalls *Gola/Schomerus*, BDSG, § 6c Rn. 2; *Bizer* in: Simitis, BDSG, § 6c Rn. 15 ff.

[518] A.A. *Scholz* in: Simitis, BDSG (2011), § 3 Rn. 274, der meint, es genüge nicht, dass eine Schnittstelle – im Falle von RFID eine Luftschnittstelle – vorhanden sei, über die ein Auslesen möglich ist. Vielmehr käme es auf eine Verarbeitung hinter der Schnittstelle, also auf dem Speichermedium an.

lichkeitsrecht des Einzelnen ging es dem Gesetzgeber bei der Schaffung von § 6c BDSG[519], stellt er doch ausdrücklich klar:

> „Mobile personenbezogene Speicher- und Verarbeitungsmedien (vgl. § 3 Abs. 10) zeichnen sich dadurch aus, dass personenbezogene Daten auf ihnen nicht nur gespeichert, sondern auch verarbeitet werden können, **ohne dass diese Verarbeitungsvorgänge für den Betroffenen unmittelbar nachvollziehbar sind** [Hervorhebung eingef. d. Verf.]."[520]

Dass es dem Gesetzgeber ausdrücklich darauf ankam, nur mittels Rechenleistung auf dem Medium selbst durchgeführte Verarbeitungsvorgänge in den Anwendungsbereich von § 6c BDSG mit aufzunehmen, lässt sich mithin nicht alternativlos in die Gesetzesbegründung hineinlesen. Vielmehr muss man vor diesem Hintergrund abweichend von der Interpretation, Medien i.S.v. § 6c BDSG müssten einen irgendwie gearteten Verarbeitungsvorgang mittels Rechenleistung eines Prozessorchips unterstützen, zu dem Ergebnis kommen, dass auch solche Medien umfasst sind, die „nur" ausgelesen werden können, sofern diese Auslesung unbemerkt vom Betroffenen stattfinden kann.

Das Auslesen kann nach dem Gesetzeswortlaut von der ausgebenden sowie anderen Stellen vorgenommen werden. Insoweit kommt es nicht darauf an, ob eine dritte Stelle autorisiert ist[521], die Daten auszulesen, vielmehr kommt es auf die faktische Möglichkeit an. Diese Stelle treffen auch die Informationspflichten aus § 6c Abs. 1 BDSG. Die ursprünglich alleine verantwortliche Stelle i.S.v. § 3 Abs. 7 BDSG – die das Speichermedium an den Betroffenen ausgegeben hat – muss demnach nicht zwangsläufig die einzige verpflichtete Stelle i.S.v. § 6c Abs. 1 BDSG bleiben – nämlich im Falle der Drittauslesung. Die dritte Stelle wird aber freilich im Moment der Auslesung selbst verantwortliche Stelle i.S.v. § 3 Abs. 7 BDSG und muss demnach auch alle weiteren Voraussetzungen, die an die Rechtmäßigkeit einer Datenverarbeitung zu stellen sind, erfüllen.

ff) Grundsatz der Datenvermeidung und Datensparsamkeit, § 3a BDSG

Der ebenfalls mit der TKG-Novelle 2001 durch § 3a BDSG eingeführte Grundsatz der Datenvermeidung und Datensparsamkeit stellt faktisch keine Rechtmäßigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten auf. Vielmehr handelt es sich um eine Zielvorgabe, mithilfe derer der Übergang von einem rein gesetzlichen zu einem Datenschutz durch Technik vorangetrieben werden soll.[522] Die Nichteinhaltung der Norm führt damit nicht zur Rechtswidrigkeit der Datenverarbeitung. Entsprechend können Verstöße auch nicht sanktioniert werden.

---

[519] A.A. *Scholz* in: Simitis, BDSG (2011), § 3 Rn. 276, der meint, mit der Regelung des § 6c BDSG habe lediglich der Intransparenz möglicher Datenverarbeitungsvorgänge durch Festlegung von Informationspflichten begegnet werden sollen. Um die aus der Intransparenz und der fehlenden Kontrollmöglichkeit resultierenden Gefahren für die informationelle Selbstbestimmung des Einzelnen sei es dem Gesetzgeber dabei nicht gegangen. Welchen Hintergrund der Gesetzgeber hingegen in einem datenschutzrechtlichen Zusammenhang sonst hätte haben können, Transparenz zu schaffen, erklärt er nicht.

[520] BDSG-ÄndG 2001, oben Fn. 512, S. 63.

[521] So aber *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 104.

[522] *Gola/Schomerus*, BDSG, § 3a Rn. 2; *Bizer* in: Simitis, BDSG, § 3a Rn. 22 ff., 36 ff.

Das Ziel, das das Gesetz vorgibt ist, dass mithilfe des Einsatzes von technischen Maßnahmen wenn möglich gar keine (Datenvermeidung) oder jedenfalls so wenig wie möglich (Datensparsamkeit) personenbezogene Daten erhoben und verarbeitet werden. Der Ansatz des Datenschutzes durch Technik wird zunehmend geprägt durch den Begriff der *Privacy Enhancing Technologies*[523].

Der Grundsatz der Datenvermeidung und Datensparsamkeit korreliert mit dem Grundsatz der Erforderlichkeit, der sich explizit in §§ 13 Abs. 1, 14 Abs. 1, 15 Abs. 1 Nr. 1, 16 Abs. 1 Nr. 1 und 20 Abs. 2 Nr. 2 BDSG für Datenverarbeitungen öffentlicher Stellen und §§ 28 Abs. 1 S. 1 Nr. 1, Nr. 2 sowie Abs. 2 Nr. 2 und 35 Abs. 2 Nr. 3 sowie Nr. 4 BDSG für Datenverarbeitungen nicht-öffentlicher Stellen wiederfindet, er geht indes nicht in ihm auf[524]. Personenbezogene Daten dürfen nach dem Erforderlichkeitsgrundsatz nur erhoben und verarbeitet werden, soweit es für den gesetzlich oder durch Einwilligung des Betroffenen legitimierten Zweck erforderlich ist. Der Grundsatz der Erforderlichkeit verbietet mithin grundsätzlich Verarbeitungsmaßnahmen personenbezogener Daten, soweit sie nicht erforderlich sind wohingegen der Grundsatz der Datenvermeidung und Datensparsamkeit die verantwortliche Stelle auch im Falle der Erforderlichkeit dazu anhält, soweit wie möglich auf anonymisierte (§ 3 Abs. 6 BDSG) oder jedenfalls pseudonymisierte (§ 3 Abs. 6a BDSG) Daten zurückzugreifen. Dies gilt für die gesamte Zeit der Lebensdauer der betroffenen Daten, die mithin regelmäßig dahingehend überprüft werden sollen, ob sie weiterhin in personenbezogener Form vorliegen müssen oder ob gegebenenfalls auch die Weiterverwendung in anonymisierter oder jedenfalls pseudonymisierter Form ausreichend zur Erreichung der verfolgten Zwecke ist.

gg) Technische Sicherheit, § 9 BDSG und Anlage

§ 9 BDSG normiert gemeinsam mit der zu Satz 1 der Regelung gehörenden Anlage das Prinzip Datenschutz durch Datensicherheit bzw. Datensicherung.[525] Durch Treffen der erforderlichen technischen und organisatorischen Maßnahmen zur Erfüllung der beispielhaft in der Anlage zu § 9 S. 1 BDSG aufgestellten Anforderungen soll eine größtmögliche Sicherheit der Daten gegen Verlust, Beschädigung und Missbrauch erreicht werden. Damit verfolgt die Norm einen grundlegend anderen Ansatz als § 3a BDSG: Mittels Technik sollen erforderliche personenbezogene Daten vor unbefugter Einflussnahme geschützt und nicht ihre Verwendung als solche vermieden oder reduziert werden. Die Anlage sieht hierbei Maßnahmen im Bereich der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle sowie die Möglichkeit der getrennten Verarbeitung von für unterschiedliche Zwecke erhobener Daten vor. Umfasst sind alle Maßnahmen, die erforderlich sind, um eine sichere und damit datenschutzgerechte Datenverarbeitung ermöglichen.

---

[523] Hierzu unten mehr E.II.1.d).

[524] *Gola/Schomerus*, BDSG, § 3a Rn. 5.

[525] Vgl. *Gola/Schomerus*, BDSG, § 9 Rn. 3.

hh) Leading Scenarios

Die oben dargestellten allgemeinen Zulässigkeitsvoraussetzungen sollen im Folgenden für die einzelnen *Leading Scenarios* überprüft werden.

aaa) Einwilligung

Szenario 1

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

Bei der Verwendung von RFID im Pass- und Ausweiswesen bedarf es bezüglich der meisten auf dem Tag zu speichernden Daten keiner Einwilligung seitens des Betroffenen: Bereits anhand der gesetzlichen Ermächtigung in § 4 Abs. 3 PassG sowie § 5 Abs. 6 PAuswG sind die Meldebehörden zur Speicherung der dort genannten Angaben auf dem RFID-Tag berechtigt und sogar verpflichtet. Beim Personalausweis werden indes – anders als beim Pass – die Fingerabdrücke des Betroffenen nur auf dessen Antrag gespeichert, § 9 Abs. 3 S. 4 PAuswG. In dem schriftlich abzugebenden Antrag kann gleichermaßen die Einwilligung i.S.d. § 4a BDSG erblickt werden.[526]

Wie bereits festgestellt richtet sich die weitere Verarbeitung der auf dem Tag gespeicherten Daten ebenfalls nach den spezialgesetzlichen Vorschriften in PassG und PAuswG. Die dort genannten Stellen dürfen für bestimmte Zwecke die Daten auslesen und verwenden. Die Verarbeitung zu anderen als den im Gesetz genannten Zwecken – durch öffentliche als auch durch nicht-öffentliche Stellen – ist auch nicht mittels Erteilung der Einwilligung durch den Betroffenen nach § 4a BDSG möglich. Die einschlägigen Gesetze sind in dieser Hinsicht abschließende Sonderregelungen[527], was sich vor dem besonderen Gefahrenpotenzial bzgl. der auf den Identifikationspapieren gespeicherten Daten erklärt.

Bei sonstigen (privatwirtschaftlichen) RFID-Anwendungen i.S.v. Szenario 1 bedarf es hingegen einer Einwilligung, sofern die Datenverarbeitung nicht bereits durch den Geschäftszweck (§ 28 BDSG) der datenverarbeitenden Stelle gerechtfertigt ist.[528] Weil – wie im Beispiel des ÖPNV-Tickets – hier regelmäßig ein Vertragsverhältnis zugrunde liegt, über das eine meist schriftliche Dokumentation vorhanden ist, wird die Einwilligung jedenfalls bzgl. der Datenverarbeitungsmaßnahmen durch die ausgebende Stelle bei Vertragsschluss erteilt werden können. Hinsichtlich sonstiger Datenverarbeitungsmaßnahmen durch Dritte – wie insbesondere in einer ubiquitären RFID-Umgebung denkbar – muss ebenfalls die Einwilligung des Betroffenen eingeholt werden, soweit nicht eine anderweitige Erlaubnisnorm – maßgeblich §§ 28 oder 30a BDSG – herangezogen werden kann. Gerade beim Abschluss eines Vertrags

[526] So wohl jedenfalls *Schulz* in: Schliesky, Gesetz über Personalausweise und den elektronischen Identitätsnachweis, § 5 Rn. 28.

[527] *Schulz* in: Schliesky, Gesetz über Personalausweise und den elektronischen Identitätsnachweis, § 14 Rn. 1.

[528] Hierzu unten D.II.2.e)aa).

kann es indes empfehlenswert sein, die Einwilligung des Betroffenen mit einzuholen: Hierdurch werden alle Zweifel an der Rechtmäßigkeit der betreffenden Datenverarbeitung zerstreut. Nichts desto trotz ermächtigt auch die Einwilligung nicht pauschal zu allen Datenverarbeitungen; der Zweckbindungsgrundsatz gilt auch hier, § 4a Abs. 1 S. 2 BDSG.

Szenario 2

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

Bei der Verwendung implantierter RFID-Tags in der Privatwirtschaft wird regelmäßig ein Vertragsverhältnis zugrunde liegen, dessen Erfüllung die Verarbeitung der auf dem Tag sowie der im Hintergrund gespeicherten Daten durch die Tag ausgebende Stelle rechtfertigen kann, s.u. zu § 28 Abs. 1 S. 1 Nr. 1 BDSG. Dass eine Implantierung im privaten Bereich ohne ein irgendwie geartetes Vertragsverhältnis stattfindet, erscheint unwahrscheinlich. Insofern wird regelmäßig – seitens der Tag ausgebenden Stelle – auf die Einholung einer Einwilligung seitens des Betroffenen verzichtet werden können. Auch hier gilt indes, dass Zweifel an der Rechtmäßigkeit bestimmter Datenverarbeitungsmaßnahmen mithilfe einer gegebenenfalls zusätzlich einzuholenden Einwilligung vermieden werden können. Für dritte datenverarbeitende Stellen, die die Identifikationsnummer in ihrer eigenen RFID-Umgebung auslesen und weiterverarbeiten wollen, kommt es auf den Einzelfall an. Auch hier ist denkbar, dass ein Vertragsverhältnis gegeben ist, welches die Datenverarbeitungen rechtfertigt – ein solches Vertragsverhältnis müsste im Zweifel so ausgestaltet sein, dass die Auslesung aller durch den Betroffenen bei sich geführten RFID-Tags erforderlich wäre. Dies dürfte in der Realität indes ein unwahrscheinliches Szenario bleiben, sodass dritte datenverarbeitende Stellen wiederum regelmäßig die Einwilligung des Betroffenen zur Verarbeitung der auf dem implantierten Tag gespeicherten Daten werden einholen müssen.

Szenario 3

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

Für die Rechtfertigung der Datenverarbeitung bzgl. Daten i.S.v. Szenario 3 gilt bei Szenario 2 gesagtes. Auch hier ist zwischen der Tag ausgebenden und dritten datenverarbeitenden Stellen zu unterscheiden. Ob das betreffende Tag implantiert ist oder aber lediglich vom Betroffenen mitgeführt wird, ändert an dieser Einschätzung nichts.

Szenario 4

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur wei-

terführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

Auch bei Szenario 4 ist zwischen der Tag ausgebenden Stelle – dem Einzelhändler, der das Produkt an den Betroffenen abgibt – und dritten datenverarbeitenden Stellen, die die Daten in ihrer eigenen RFID-Umgebung auslesen, zu unterscheiden. Indes stellt sich hier die Besonderheit dar, dass der Betroffene nicht bereits vor der Erlangung des getaggten Gegenstandes im Wege eines Vertragsformulars o.ä. auf die Gegenwart der RFID-Infrastruktur aufmerksam gemacht wird und folglich – mangels Kenntnis – auch keine wirksame Einwilligung – schon gar keine schriftliche – abgeben kann. Gleichfalls wäre die Einholung der schriftlichen Einwilligung von jedem mit der RFID-Technik in Berührung kommenden Kunden praktisch unmöglich – nicht nur würde es seitens des Betreibers einen nicht zu überblickenden Aufwand erfordern, ein solches Vorgehen würde von den Kunden auch kaum angenommen werden.

Bereits wegen des Schriftformerfordernisses wird die Einwilligungslösung nur in den RFID-Anwendungen zum Tragen kommen können, in die sich die Betroffenen ohnehin freiwillig und in Kenntnis der Sachlage begeben. Umso dringlicher stellt sich bei RFID-Anwendungen i.S.v. Szenario 4 die Frage der sonstigen Rechtfertigung mittels Erlaubnistatbestand, maßgeblich §§ 28 Abs. 1 sowie 30a BDSG.

bbb) Direkterhebungsgrundsatz

Szenario 1

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

Hinsichtlich des Direkterhebungsgrundsatzes gilt zunächst ganz grundsätzlich: RFID-Anwendungen, in denen der Betroffene den Datenübertragungsvorgang selbst initiiert, begegnen keinen Schwierigkeiten im Hinblick auf den Direkterhebungsgrundsatz. Sofern die Datenübertragung indes ohne sein aktives Zutun erfolgt, kommt einerseits eine Rechtfertigung mittels ausdrücklicher und bewusster Duldung oder aber im Wege einer gesetzlichen Ausnahme in Betracht.

Für Anwendungen i.S.v. Szenario 1 bedeutet dies, dass bei bewusstem Einsatz des RFID-Tags – bei Ausweispapieren z.B. bei der Aushändigung selbiger an die zuständigen Behördenmitarbeiter, bei ÖPNV-Tickets beim Einsteige- und Autorisierungsvorgang in einem Nahverkehrsmittel – dem Direkterhebungsgrundsatz entsprochen wird. Bei diesen „bestimmungsgemäßen“ Auslesevorgängen geht es für den Betroffenen regelmäßig darum, eine „Gegenleistung“ für die Preisgabe seiner Daten zu bekommen – die Erlaubnis, am Flughafen nach Deutschland einreisen zu können oder die U-Bahn benutzen zu dürfen. Die Erforderlichkeit der Datenauslesung ist damit deutlich und der Betroffene trifft eine bewusste und informierte Entscheidung. Weil ihm die datenerhebende Stelle zudem bekannt ist, ist ihm die Möglichkeit gegeben, von seinen Betroffenenrechten Gebrauch zu machen.

Szenario 2

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

In Anwendungsfällen zu Szenario 2 ergibt sich ein vergleichbares Bild: Auch mittels implantiertem RFID-Tag kann sich der Betroffene in bestimmten Situationen identifizieren und damit Zugangsschranken überwinden – so z.B. im Baja Beachclub. Die entsprechenden Auslesevorgänge werden ebenfalls von ihm initiiert. Die im Hintergrundsystem gespeicherten Daten sind regelmäßig gegen unbefugten Zugriff geschützt. Selbst mit der RFID-Identifikationsnummer als „Schlüssel" kann unter normalen Umständen ein Dritter nicht auf die Hintergrunddaten zugreifen. Die Identifikationsnummer hingegen kann er – soweit diese nicht verschlüsselt ist – auslesen, um damit z.B. ein Bewegungsprofil anzulegen. Sofern eine solche Auslesung versteckt, also ohne Kenntnis des Betroffenen und damit ohne sein Zutun erfolgt, ist eine Rechtfertigung der Auslesung nur über eine der Ausnahmen in § 4 Abs. 2 S. 2 BDSG (hierzu sogleich mehr) möglich.

Szenario 3

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

Auch bei RFID-Anwendungen i.S.v. Szenario 3 sind Situationen wahrscheinlich, in denen der Betroffene den Auslesevorgang initiiert: Seine Kundenkarte wird er – sofern er treuer Punktesammler ist – freiwillig bei jedem Bezahlvorgang bei einem der teilnehmenden Unternehmen vorzeigen und seine Daten erheben lassen. Weitergehende Auslesevorgänge in den Räumlichkeiten der teilnehmenden Unternehmen – zum Anlegen von Kundenprofilen – finden jedenfalls ohne aktives Zutun des Betroffenen statt. Sofern er indes bei Aushändigung der Kundenkarte auf die Möglichkeit der Profilierung zu Geschäftsoptimierungszwecken und zwecks passgenauer Werbeangebote auf diese Auslesevorgänge aufmerksam gemacht worden ist, duldet der Betroffene diese bewusst. Allerdings muss ihm zuvor die Möglichkeit eingeräumt worden sein, solchen Auslesevorgängen zu widersprechen. Denn eine erzwungene Duldung, der man allenfalls unter Ausschlagung des gesamten Angebots sprich Verzichts auf die Kundenkarte insgesamt entgehen kann, entspricht nicht mehr dem Direkterhebungsgrundsatz (Kopplungsverbot). Sollte eine solche Ablehnungsmöglichkeit nicht gegeben sein – was unter Umständen technisch oder wirtschaftlich für das Unternehmen unmöglich sein kann – muss wiederum eine der Ausnahmen aus § 4 Abs. 2 S. 2 BDSG einschlägig sein.

Szenario 4

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur wei-

terführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

Die Auslesung von RFID-Tags i.S.v. Szenario 4 wird regelmäßig nicht auf Initiative des Betroffenen stattfinden. Allenfalls beim Bezahlvorgang im Pulk erfassenden Kassensystem wird man von der Initiative des Betroffenen und damit seiner Mitwirkung ausgehen können. Bei sonstigen auf der Verkaufsfläche stattfindenden Auslesevorgängen, die unbemerkt vom Betroffenen stattfinden – wiederum vom Betreiber durchgeführt zwecks Anlegung von Bewegungs- und Kundenprofilen sowie passgenauer Werbemaßnahmen – ist eine aktive Mitwirkung zu verneinen. Auf eine aktive Mitwirkung des Betroffenen werden es die Unternehmen ohnehin nicht ankommen lassen, wollen sie doch gerade verhindern, dass die Betroffenen – direkt zur Datenhingabe aufgefordert – sich selbiger verweigern. Stattdessen dürfte zu erwarten sein, dass die Betreiber zunächst auf die ausdrückliche und bewusste Duldung des Betroffenen setzen. Dies setzt voraus, dass der Betroffene umfassend über die Datenerhebung informiert ist, also über die Identität der datenverarbeitenden Stelle, den Zweck der Erhebung, der Verarbeitung und der Nutzung der Daten sowie die Kategorien von Empfängern, sofern eine Übermittlung der Daten an Dritte geplant ist, § 4 Abs. 3 S. 1 BDSG. Wenn es dem Betreiber nicht gelingt, diese Information an den Betroffenen zu vermitteln, ist dieser nicht umfassend informiert und seine Duldung nicht bewusst. In der Praxis dürfte sich eine solch umfassende Information des Betroffenen als äußerst umständlich darstellen: Wegen des Gefährdungspotenzials müssen schließlich hohe Anforderungen an die entsprechende Information gestellt werden. Die datenverarbeitende Stelle darf nicht leichtfertig von der Kenntnis des Betroffenen von den erforderlichen Informationen ausgehen.[529] Vielmehr muss der Betroffene so umfassend informiert werden, dass er von seinen gesetzlichen Rechten effektiv Gebrauch machen kann.[530] Dies hieße, dass jeder Kunde bei jedem Supermarktbesuch o.ä. über die vorhandene RFID-Infrastruktur und die mit der Datenauslesung verbundenen Ziele aufgeklärt werden müsste. Dies dürfte mittels massentauglicher sprich entsprechend optisch gestalteter Warnhinweise schwer umzusetzen sein.[531]

Doch selbst wenn eine solch umfassende Information an den Betroffenen gelingen sollte, die dem Maßstab der bewussten Duldung genügt, so stellt sich doch weiter die Frage, ob der Betroffene eine tatsächliche Möglichkeit zur Entziehung hat. Nur wer eine Wahlmöglichkeit hat, kann sich einer von ihm nicht gewollten Situation entziehen. In einer Welt ubiquitärer RFID-Anwendungen ist dies äußerst unwahrscheinlich: Sofern RFID globaler Standard in der Produktidentifikation und entsprechend flächendeckend im Einzelhandel eingesetzt wird, verbleibt dem Einzelnen keine Möglichkeit mehr sich im Wege der Entziehung vor den Auswirkungen von RFID-Anwendungen zu schützen. Zwar setzt dies technische Standards voraus, denn ohne Kompatibilität der einzelnen Systemkomponenten droht auch keine Fremdausle-

[529] *Sokol* in: Simitis, BDSG, § 4, Rn. 40.

[530] *Gola/Schomerus*, BDSG, § 4 Rn. 30 ff.

[531] Einen entsprechenden Vorstoß hat indes die Europäische Kommission in ihrer Empfehlung 2009/387/EG, oben Fn. 2, vorgenommen. Dazu mehr unten E.II.1.

sung der RFID-Tags. Standardisierungsbestrebungen bestehen allerdings[532] und werden sich wahrscheinlich jedenfalls auf Produktebene vergleichbar dem EAN-Code durchsetzen. Die bewusste Duldung wird damit unterminiert und bedeutungslos. Die Konsequenz kann nur sein, dass selbst bei hinreichender Aufklärung des Einzelnen eine Erhebung bei ihm ohne seine Mitwirkung stattfindet. Der Direkterhebungsgrundsatz wäre damit verletzt und es bedürfte einer gesetzlichen Ausnahmeerlaubnis gem. § 4 Abs. 2 S. 2 BDSG unter Einbeziehung der schutzwürdigen Interessen des Betroffenen.

Die erreichbare Lesereichweite spielt in diesem Zusammenhang nur eine untergeordnete Rolle: Zwar wird die unbemerkte Auslesung bei NFC-Technik o.ä. deutlich erschwert, sie wird indes nicht unmöglich. Es kommt also auch bei solchen Anwendungen konkret darauf an, ob Daten ausgelesen werden und ob der Betroffene den Auslesevorgang (mit)steuert.

Für die Fälle der Profilbildung könnten die zwei Ausnahmetatbestände in § 4 Abs. 2 S. 2 Nr. 2 a) und b) BDSG herangezogen werden. An beide Ausnahmetatbestände sind hohe Anforderungen zu stellen.[533] Die erste Ausnahme, Erforderlichkeit der Datenerhebung wegen des Geschäftszwecks, ist denknotwendigerweise nur einschlägig in Fällen, in denen eine Erhebung der Daten beim Betroffenen selbst den Geschäftszweck zu vereiteln drohte.[534] Dies ist bei der Erhebung von RFID-Tag Daten zu Zwecken der Profilbildung nicht der Fall: Eine Vertragsbeziehung im Einzelhandel hängt nicht davon ab, dass der Geschäftspartner zunächst ein umfassendes Profil des potenziellen Kunden anlegt. Dies kann lediglich dann gelten, wenn die Gegenleistung gerade davon abhängt, dass ein Nutzerprofil angelegt wird. In solchen Fällen dürfte aber die Erhebung schon unter Mitwirkung des Betroffenen, nämlich mit seiner bewussten Duldung, stattfinden.

Möglicherweise wäre aber die Erhebung dennoch gerechtfertigt, weil eine Mitwirkungshandlung – bzw. vollumfängliche Information – des Betroffenen einen unverhältnismäßigen Aufwand darstellte. Wie bereits angesprochen, wäre eine aktive Mitwirkung des Betroffenen höchst impraktikabel und würde von potenziellen Kunden sicherlich abgelehnt. Die umfassende Information des Betroffenen könnte indes tatsächlich als unverhältnismäßiger Aufwand angesehen werden, bedenkt man, dass die datenverarbeitende Stelle sich der Kenntnis des Betroffenen sicher sein muss.[535] Sicherheit könnte nur erlangt werden, wenn jeder Kunde vor dem Betreten des Geschäfts über seinen Kenntnisstand befragt würde. Dies ist lebensfremd und kann aus praktischen Gesichtspunkten nicht zu fordern sein. Damit stellt die Erhebung unter bewusster Duldung des Betroffenen tatsächlich einen unverhältnismäßigen Aufwand dar.

---

[532] Vgl. zu den EPC-Standards oben C.I.1.

[533] *Sokol* in: Simitis, BDSG, § 4 Rn. 34 und 35.

[534] Z.B. bei Unerreichbarkeit des Betroffenen oder der Überprüfung von Angaben des Betroffenen zur Kreditwürdigkeit

[535] Vgl. die parallele Wertung zum Kenntnisbegriff in § 4 Abs. 3 S. 1 BDSG bei *Sokol* in: Simitis, BDSG, § 4 Rn. 40.

Allerdings müssen eventuelle schutzwürdige Interessen des Betroffenen berücksichtigt werden. Bestehen Anhaltspunkte, dass ein solches in überwiegendem Maße vorhanden ist, genügt auch das Vorliegen des Ausnahmetatbestandes nicht für die Rechtfertigung der Datenerhebung. Eine Beeinträchtigung der Interessen des Betroffenen kann durch die Art der Datenerhebung erfolgen als auch wegen der Person oder Stelle, bei der die Daten erhoben werden sollen.[536] Grundsätzlich kommt es auf den Verwendungszusammenhang, in dem die Daten erhoben werden, an und es muss eine Abwägung mit den Interessen der datenverarbeitenden Stelle vorgenommen werden.[537] Das Ergebnis dieser Abwägung wird in verschiedenen RFID-Anwendungen unterschiedlich ausfallen. Stellte man zwei Extreme gegenüber, so wären die schutzwürdigen Interessen des Betroffenen an einer Nichterhebung der RFID-Daten im Gesundheitssektor als eher niedrig einzustufen. Vielmehr wird er sich gerade aus Sicherheits- oder Gesundheitsgründen in einer RFID-Umgebung – Krankenhaus, Altersheim – befinden. Um Notfallsituationen sicher zu erkennen, ist eine fortwährende Erhebung der RFID-Daten im Chip des Patienten erforderlich und das Interesse der datenverarbeitenden Stelle überwiegt. Im Einzelhandel hingegen sieht die Interessenlage anders aus. Der datenverarbeitenden Stelle liegt viel daran, Kundenprofile erstellen zu können.[538] Zwar bekommt der Betroffene im Gegenzug auch etwas geboten – z.B. kundensensitive Werbung – der tatsächliche Mehrwert für den Einzelnen variiert hingegen und ist für die datenverarbeitende Stelle nicht erkennbar. Unterschiedlich wird auch das Interesse des jeweiligen Betroffenen sein, nicht profiliert zu werden: Während sich viele Menschen hieran nicht stören werden, wird es anderen ein Gefühl der Überwachung vermitteln, der sie sich möglichst entziehen wollen. Diese Interessenlage ist für die datenverarbeitende Stelle solange undurchsichtig, solange ein Betroffener nicht ausdrücklich der Profilierung widerspricht. Andersherum kann dies aber nicht heißen, dass die datenverarbeitende Stelle solange vom Nichtvorliegen überwiegender schutzwürdiger Interessen beim Betroffenen ausgehen darf, solange dieser sich nicht aktiv wehrt. Dies konterkarierte das Ziel des Ausnahmetatbestandes. Eine praxisnahe Lösung könnte durch Zusammenwirken beider Akteure erzielt werden, z.B. in einer Kombination aus Warnhinweisen beim Betreten einer RFID-Umgebung und dem Hinweis auf die Möglichkeit weitergehende Informationen auf Nachfrage zu erhalten und dann ggf. zu widersprechen.

Bereits die Einhaltung des Direkterhebungsgrundsatzes wird sich dementsprechend in vielen RFID-Anwendungen und insbesondere in einer ubiquitären RFID-Umgebung – vornehmlich infolge der umfassenden Infrastruktur im Einzelhandel – als schwierig darstellen. Festzuhalten bleibt, dass bei flächendeckendem, weitgehend standardisiertem Einsatz von RFID auf Produktebene die Erhebung solcher RFID-Produktidentifikationsnummern an die Grenzen der in § 4 Abs. 2 BDSG geschaffenen Möglichkeiten für eine legitime Erhebung der Daten – entweder direkt beim Betroffenen oder aber ohne seine Mitwirkung – stoßen werden. Solange kein flächendeckender Einsatz gegeben ist, werden sich Betreiber von RFID-Anwendungen ggf. mittels umfassender Information der Betroffenen auf deren bewusste Duldung berufen

[536] *Sokol* in: Simitis, BDSG, § 4, Rn. 36.

[537] *Sokol* in: Simitis, BDSG, § 4, Rn. 37.

[538] Vgl. hierzu oben C.II.2.

können. Dies kann indes nicht mehr gelten, wenn den Betroffenen in einer ubiquitären RFID-Umgebung keine Entziehungsmöglichkeit mehr verbleibt.

Die Ausnahmeregelungen in § 4 Abs. 2 S. 2 BDSG können in einigen RFID-Anwendungen herangezogen werden, in dem kritischen Szenario der Profilbildung im Einzelhandel hingegen dürfte es schwer sein, ein überwiegendes Interesse der datenverarbeitenden Stelle an der Datenerhebung gegenüber den schutzwürdigen Interessen des Betroffenen an der Nicht-Erhebung zu begründen.

ccc) Datenübermittlung ins Ausland

Die Datenübermittlung ins Ausland wird eine zunehmend größer werdende Rolle auch im Zusammenhang mit RFID-Anwendungen gewinnen. Global agierende Unternehmen – als Beispiel sei hier für den Bereich des Einzelhandels nur die METRO Group genannt – sind besonders interessiert an der flächendeckenden Einführung von RFID. Aber auch bei kleineren, national agierenden Unternehmen kann und wird es im Zuge von *Cloud Computing* verstärkt zu Datentransfers auch außerhalb der Grenzen Deutschlands und der EU/EWG kommen. Der internationale Datentransfer kann entsprechend RFID-Anwendungen aller *Leading Scenarios* betreffen. Sofern ein grenzüberschreitender Transfer stattfinden soll, muss die verantwortliche Stelle daher die Vorgaben der §§ 4b und 4c BDSG beachten und bei einem Datentransfer in Drittstaaten ein angemessenes Datenschutzniveau beim Empfänger garantieren.

ddd) Mobile personenbezogene Speicher- und Verarbeitungsmedien

Nach obigen Ausführungen zu § 6c BDSG dürften alle RFID-Tags unter dessen Anwendungsbereich fallen: Da es nach diesseitiger Ansicht nicht auf prozessorgestützte Verarbeitungen auf dem Tag selbst ankommt, sondern vielmehr die bloße Auslesbarkeit – unbemerkt vom Betroffenen – ausreicht, um den Anwendungsbereich zu eröffnen, müssen die verantwortlichen Stellen – also alle Stellen, die die Daten fernauslesen wollen – den Betroffenen über die in § 6c Abs. 1 BDSG genannten Punkte unterrichten.

Einen solchen Ansatz verfolgt auch die Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID- gestützten Anwendungen[539]. Die dort geforderte Informationspflicht entspricht weitestgehend den Anforderungen des § 6c Abs. 1 BDSG. Speziell für den Einzelhandel soll nach der Empfehlung ein gemeinsames Zeichen entwickelt werden, mittels dessen die Kunden über die Präsenz einer RFID-Infrastruktur informiert werden können.[540]

Betroffen wären alle RFID-Anwendungen und alle Stellen, die im Rahmen einer vertraglichen Beziehung zum Betroffenen oder aus jedem sonstigen Grund RFID-Tag Daten auslesen wollen. Ausgeschlossen wäre die Informationspflicht nur, soweit der Betroffene bereits Kenntnis vom Vorhandensein der RFID-Infrastruktur hat.

---

[539] Empfehlung 2009/387/EG, oben Fn. 2.

[540] Hierzu mehr unten E.II.1.

eee) Grundsatz der Datenvermeidung und Datensparsamkeit

Vor dem Hintergrund des Grundsatzes der Datenvermeidung und Datensparsamkeit hat jede verantwortliche Stelle über den gesamten Zeitraum, in dem personenbezogene Daten erhoben, gespeichert und verarbeitet werden zu prüfen, ob der Personenbezug für die Erfüllung des angestrebten Zwecks erforderlich ist. Sofern dies nicht (mehr) der Fall ist, sind die Daten zu anonymisieren bzw. pseudonymisieren soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Szenario 1

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

In den Ausweisanwendungen des Szenario 1 entfällt das Erfordernis des Personenbezugs regemäßig mit dem Erhalt eines neuen Ausweisdokuments. Sofern die Meldebehörde auf Abgabe des abgelaufenen Ausweisdokuments verzichtet, § 27 Abs. 1 Nr. 2 PAuswG, § 15 Nr. 2 PassG, müssen dann jedenfalls die Daten auf dem Tag unwiederbringlich gelöscht bzw. das Tag zerstört werden. Dies dürfte über die ohnehin bestehende Pflicht zur Kennzeichnung des alten Dokuments[541] als ungültig hinausgehen.

Die gleiche Pflicht besteht für das ÖPNV-Unternehmen, wenn das Ticket entweder erneuert wird oder aber der Betroffene den Beförderungsvertrag mit dem Unternehmen kündigt bzw. nicht verlängert. In diesen Fällen besteht kein Bedarf mehr an den auf dem Ticket gespeicherten Daten, sodass diese zu löschen sind. Dies ergibt sich bereits aus § 35 Abs. 2 S. 2 Nr. 1 BDSG. Allerdings stellt sich insbesondere im Beförderungswesen die Frage, ob auf dem Tag überhaupt personenbezogene Daten gespeichert sein müssen. Bei übertragbaren Tickets dürfte dies von vornherein zu verneinen sein. Den einzigen Beweis, den der Fahrgast bei Fahrtantritt erbringen muss, ist die Berechtigung zum Nutzen des Verkehrsmittels, sprich, ob ein gültiger Fahrausweis vorliegt. Hierfür genügt die bloße Unterscheidung: gültig oder nicht gültig. Weder eine (unverschlüsselte) Identifikationsnummer noch weitergehende Daten wie Name, Anschrift etc. sind hierfür erforderlich. Anders dürfte es sich lediglich bei unübertragbaren Tickets darstellen, weil hier im konkreten Fall überprüfbar sein muss, ob der jeweilige Fahrgast auch der berechtigte Ticketinhaber ist, etwa durch Abgleichung der Daten auf einem Ausweispapier mit den Daten auf dem Ticket. Ausreichend hierfür dürfte indes regelmäßig der Name, ggf. in Kombination mit einem weiteren Identifikationsmerkmal sein. Ein umfassender Datensatz inkl. eindeutiger Identifikationsnummer dürfte nicht erforderlich sein. Letztere Daten müssten folglich jedenfalls pseudonymisiert werden.

Eine Anonymisierung nach Entfall der Erforderlichkeit kommt in beiden Fällen wohl in Betracht, dürfte aber aus wirtschaftlicher Sicht keinen Sinn machen, wird doch die Anonymisierung jedenfalls nicht günstiger sein als die unmittelbare Zerstörung des Tags.

[541] *Schulz* in: Schliesky, Gesetz über Personalausweise und den elektronischen Identitätsnachweis, § 4 Rn. 2.

Sofern Dritte die Daten der betreffenden Tags erlaubterweise ausgelesen und verarbeitet haben, stellt sich auch bei diesen die Frage, ob die Daten in personenbezogener Form vorliegen müssen, um den zugrunde liegenden Zweck zu erreichen. Hier muss eine einzelfallspezifische Betrachtung angestellt werden.

Szenario 2

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

Die auf einem implantierten RFID-Tag gespeicherte Identifikationsnummer wird regelmäßig in anonymisierter Form keinen Sinn machen, liegt das zu erreichende Ziel doch in der zweifelsfreien Identifikation des Betroffenen – dies gilt sowohl in medizinisch indizierten Anwendungen als auch bei der „implantierten Geldbörse". Eine Pseudonymisierung ist hingegen denkbar, behält doch die autorisierte Stelle den Schlüssel, um die eindeutige Identifizierung weiterhin durchführen zu können. Auch die im Hintergrundsystem abgelegten weitergehenden Informationen müssen so lange mit Personenbezug gespeichert sein, wie der zugrunde liegende Zweck – also z.B. der Behandlungsvertrag – besteht. Entfällt dieser, besteht grundsätzlich auch kein Erfordernis mehr an personenbezogenen Daten und zwar weder auf dem RFID-Tag noch im Hintergrundsystem. Die Löschungspflicht ergibt sich wiederum regelmäßig aus § 35 Abs. 2 S. 2 Nr. 1 BDSG. Im Gesundheitssektor ist indes zu berücksichtigen, dass jedenfalls die im Hintergrundsystem gespeicherten Daten gewissen Archivierungspflichten unterliegen können und dementsprechend jedenfalls in pseudonymisierter Form gespeichert bleiben müssen. In diesem Fall sind die Daten gem. § 35 Abs. 3 Nr. 1 BDSG gegen unbefugten Zugriff zu sperren.

Szenario 3

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

Auch bei Kundenkarten kommt es maßgeblich auf das zugrundeliegende Vertragsverhältnis an: Besteht es, hat die verantwortliche Stelle auch einen Bedarf an personenbezogenen Daten und zwar sowohl in Form der auf dem Tag gespeicherten Identifikationsnummer als auch hinsichtlich der im Hintergrundsystem gespeicherten weitergehenden Daten. Besteht es nicht mehr, ist zunächst ohnehin zu prüfen, ob eine weitergehende Verarbeitung der betroffenen personenbezogenen Daten – wie z.B. zur weitergehenden Profilierung des Betroffenen – noch durch einen Erlaubnistatbestand gerechtfertigt ist. Ist sie dies nicht, ergibt sich bereits eine Löschungspflicht aus § 35 Abs. 2 S. 2 Nr. 1 BDSG. Ist sie es indes, so kommt es weiterhin maßgeblich darauf an, ob der verfolgte Zweck auch mit Daten ohne Personenbezug erreicht werden kann. Bei personengenauen Profilen – also nicht Profilen von Vergleichsgruppen o.ä. – wird dies zu bejahen sein.

Szenario 4

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur weiterführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

Nachdem, wie oben festgestellt, auch bloße Produktidentifikationsnummern als personenbezogene Daten zu qualifizieren sind, sofern sie von Personen mitgeführt werden, gilt es in Szenario 4 besonderes Augenmerk auf die Einhaltung des Grundsatzes der Datenvermeidung und Datensparsamkeit zu legen. Der Personenbezug ist für die verantwortliche Stelle in diesem Szenario – wenn man einmal von etwaigen elektronischen Garantien absieht – aus einem Grund von Interesse: Der Anlegung von möglichst umfangreichen und spezifischen Kundenprofilen. Bei Einwegprodukten wie Lebensmitteln ist dieses Potenzial gering, können ihre Tag-Daten doch nur beim aktuellen Einkauf zur Erstellung solcher Profile verwendet werden. Bei Mehrwegprodukten wie der Brille oder dem Portemonnaie hingegen lassen sich über die Zeit sehr umfangreiche auf eine Person bezogene Profile erstellen. Zu eben dieser personengenauen Profilierung sind wie bereits erwähnt auch Daten mit Personenbezug erforderlich. Dringlicher stellt sich in diesen Fällen die Frage, ob die Datenerhebung zum alleinigen Zweck der Profilierung überhaupt gerechtfertigt ist. Dies wird sogleich besprochen.[542] Der Grundsatz der Datenvermeidung und Datensparsamkeit tritt hier etwas in den Hintergrund und ändert im Ergebnis auch nichts an der abschließenden Einschätzung: Ist die Profilierung erlaubt, so ist auch die Verwendung von Daten im nicht-pseudonymisierten Zustand erforderlich. Ist sie es nicht, so bedarf es auch keiner personenbezogenen Daten, dann muss die verantwortliche Stelle die Daten bereits bei der Auslesung anonymisieren.

fff) Technische Sicherheit

Infolge der Vorgaben des § 9 BDSG in Kombination mit der Anlage müssen die verantwortlichen Stellen die in RFID-Anwendungen verarbeiteten Daten und die verwendeten technischen Infrastrukturen vor dem Zugriff und der Einflussnahme durch Unbefugte schützen.

Im Rahmen der Zutrittskontrolle bedeutet dies, dass die verantwortliche Stelle dafür Sorge zu tragen hat, dass kein Unbefugter in die räumliche Nähe jedwelcher technischer Geräte der RFID-Anwendung gelangen kann. Vor diesem Hintergrund erklärt sich auch die Verfügung des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), die Kartenlesegeräte für die neue elektronische Gesundheitskarte nur in einer Einsatzumgebung aufzustellen, in der die Geräte nicht länger als 30 Minuten unbeaufsichtigt sind; sofern diese 30-Minuten-Spanne nicht eingehalten werden kann, müssen die Geräte auf ihre Unversehrtheit überprüft werden.[543] An diesem Beispiel zeigt sich, wie schwierig es sein kann, eine hinreichende Zutrittskontrolle zu gewährleisten. Systemkomponenten, bei denen personenbezogene Daten unmit-

[542] S. unten D.II.2.e)aa).

[543] Heise News Meldung vom 15.05.2011, BSI verärgert Ärzte, abrufbar unter http://www.heise.de/newsticker/meldung/BSI-veraergert-Aerzte-1243157.html (04.04.2013).

telbar eingesehen werden können, wie Computerbildschirme, sind entsprechend noch strenger zu schützen.

Im Rahmen der Zugriffskontrolle hat die verantwortliche Stelle darüber hinaus sicherzustellen, dass Unbefugte keinen Zugriff auf die in einem RFID-System gespeicherten Daten erhalten. Zum RFID-System gehört auch das RFID-Tag, welches an den Betroffenen ausgegeben wird. Um zu verhindern, dass ein Dritter ohne Berechtigung auf die auf dem Tag gespeicherten Daten zugreifen kann, muss die verantwortliche Stelle mithin das Erforderliche tun. In der Konsequenz hieße dies, dass alle RFID-Tags bzw. die auf ihnen gespeicherten Inhalte so geschützt werden müssen, dass ein unbefugtes Auslesen unmöglich ist oder jedenfalls nicht mehr zu einer Persönlichkeitsrechtsverletzung des Betroffenen führen kann.[544] Dies kann beispielsweise durch Verschlüsselung und damit Unkenntlichmachung der gespeicherten Daten erreicht werden.[545]

Im Übrigen gelten für RFID-Systeme vergleichbare Anforderungen wie in anderen IT-Systemen, in denen personenbezogene Daten verarbeitet werden.[546]

Bei der Speicherung personenbezogener Daten auf elektronischen Ausweisdokumenten, ist ein maximales Maß an Sicherheitsvorkehrungen erforderlich, um die Daten gegen unbefugtes Auslesen zu schützen. Aufgrund der auf dem Tag im Reisepass gespeicherten Daten würde bereits ein einziger unberechtigter Lesevorgang genügen, um den entsprechenden Menschen zu „durchleuchten", weil viele wesentliche personenbezogene Daten in Erfahrung gebracht würden. Hierauf haben der europäische und deutsche Gesetzgeber reagiert und spezielle Anforderungen an die technische Sicherheit von RFID-Tags in Ausweisdokumenten formuliert.

Der europäische Gesetzgeber hat in seiner Verordnung (EG) Nr. 2252/2004 einen sehr unbestimmten Maßstab für die Gewährleistung von Schutz und Sicherheit der gespeicherten Daten vorgegeben:

> Art. 1 Abs. 2 S. 2 der Verordnung (EG) Nr. 2252/2004
>
> Die Daten **sind zu sichern**, und das Speichermedium muss eine ausreichende Kapazität aufweisen und **geeignet sein, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen**. [Hervorhebung eingef. d. Verf.]

Der deutsche Gesetzgeber hat dies im geänderten Passgesetz folgendermaßen umgesetzt:

> § 4 Abs. 3 S. 2 PassG
>
> Die gespeicherten Daten sind gegen unbefugtes Auslesen, Verändern und Löschen zu sichern. (…)

Beide Normen sind damit technikneutral gehalten. Die RFID-Tags auf deutschen ePässen sind infolge der Regelung und dem Bedürfnis nach größtmöglicher Datensicherheit nur auslesbar, wenn zuvor die weiterhin enthaltene maschinenlesbare Zone[547] optisch eingelesen wurde. Ist

---

[544] Vgl. *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 114 f.

[545] Vgl. hierzu unten E.II.4.

[546] Vgl. weitergehend *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 110 ff.; *Gola/Schomerus*, BDSG, § 9 Rn. 22 ff.

[547] In der „machine readable zone" sind zwei Textzeilen mit Name, Geschlecht, Passnummer sowie Ausstellungs- und Ablaufdatum des Passes abgedruckt.

dies geschehen, wird der für jedes Tag speziell zu berechnende Zugriffsschlüssel ermittelt. Erst dann kann auf die Tag-Daten zugegriffen werden. Die in den Pässen enthaltenden Chips haben eine einem Pentium 1 Prozessor vergleichbare Rechenleistung und verarbeiten kryptographische Algorithmen.[548] Die maximale Lesereichweite liegt aufgrund der verwendeten niedrigen Frequenz von 13,56 MHz (*Near-Field-Communication*) bei ca. 10 cm.[549] Ein Auffinden einer bestimmten Person in einer Menschenmenge durch „Scannen" ihres ePasses ist insofern und aufgrund der eingearbeiteten Sicherheitsmechanismen fast ausgeschlossen. Um jeder Gefahr des unbefugten Auslesens des Tags zu entgehen, bietet es sich dennoch an, den Pass zusätzlich in eine Hülle aus Aluminium, welches Leseversuche vollständig abblockt, einzupacken. Ein Tracking der den Pass bei sich führenden Person wird durch verwenden von variablen MetaIDs verhindert.[550] Die vom Chip auf dem Pass gespeicherte Seriennummer wird durch ein Zufallsverfahren erzeugt.[551]

d) Besondere Regelungen für die Datenverarbeitungen öffentlicher Stellen

Nach dem allgemeinen Grundsatz des Verbots mit Erlaubnisvorbehalt in § 4 Abs. 1 BDSG muss für jede Datenverarbeitung ein Erlaubnistatbestand vorliegen. Soweit keine wirksame Einwilligung des Betroffenen gem. § 4a BDSG oder eine sonstige gesetzliche Erlaubnis gegeben ist, kann die Datenverarbeitung gegebenenfalls über die im BDSG geregelten Erlaubnistatbestände gerechtfertigt sein. Die Erlaubnistatbestände für die Datenverarbeitung durch öffentliche Stellen finden sich in §§ 13 ff. BDSG. Die in dieser Arbeit zugrunde gelegten *Leading Scenarios* sind bereits jetzt teilweise auch im öffentlichen Bereich zu verorten: Pass und Personalausweis werden von Behörden ausgegeben, Mitarbeiter im öffentlichen Dienst erhalten RFID-Tokens als Türöffner und „Stechkarte". Während sich die Ausgabe der Ausweispapiere und die Erhebung und Verarbeitung der auf ihnen gespeicherten Daten wie oben festgestellt nach den einschlägigen Gesetzen (PAuswG und PassG) richten, ist die Ausgabe von RFID-Tags insbesondere in öffentlich-rechtlichen Beschäftigungsverhältnissen mangels einschlägiger spezialgesetzlicher Normen an den allgemeinen Bestimmungen des BDSG zu messen. In diesem Zusammenhang werden eine besondere Rolle die erwarteten Änderungen zum Arbeitnehmerdatenschutz in § 32 sowie den neu einzufügenden §§ 32a ff. BDSG spielen. Diese – noch nicht verabschiedeten – Vorschriften werden indes nicht Gegenstand der folgenden Analyse sein.

Die Vorschriften des BDSG gelten ausweislich § 12 BDSG für alle öffentlichen Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen sowie teilweise für öffentliche Stellen der Länder. Die Vorschrift deckt sich mit § 1 Abs. 2 BDSG, der die generelle Anwendbarkeit des BDSG regelt.

---

[548] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 25.

[549] *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 177.

[550] Vgl. hierzu unten E.II.4.d).

[551] *Finkenzeller*, RFID-Handbuch, S. 405.

Neben den Erlaubnistatbeständen finden sich in Unterabschnitt Zwei auch Vorschriften über die Rechte des Betroffenen bei der Datenverarbeitung durch öffentliche Stellen.

aa) Erlaubnistatbestände

Bei der Datenverarbeitung durch öffentliche Stellen unterscheidet das Gesetz anders als bei Datenverarbeitungen durch nicht-öffentliche Stellen zwischen verschiedenen Formen der Datenverarbeitung und stellt diese jeweils unter unterschiedliche Rechtmäßigkeitsanforderungen. § 13 regelt allgemein die Datenerhebung, § 14 die Datenspeicherung, -veränderung und -nutzung, § 15 die Datenübermittlung an öffentliche Stellen und § 16 die Datenübermittlung an nicht-öffentliche Stellen. Die Erlaubnistatbestände rechtfertigen die jeweilige Datenverarbeitung zunächst, soweit diese für die Erfüllung der in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgaben erforderlich ist. Hierbei muss es sich um eine durch Gesetz oder durch einschlägige Verwaltungsnorm vorgeschriebene öffentlich-rechtliche Aufgabe handeln.[552] Um dem strengen Erfordernis der Erforderlichkeit gerecht zu werden, dürfen nur solche personenbezogenen Daten erhoben oder verarbeitet werden, ohne die die öffentliche Stelle ihre gesetzlichen Aufgaben nicht, nicht vollständig oder nicht in rechtmäßiger Weise durchführen können; eine Erhebung aus Dienlichkeits- oder Praktikabilitätsgründen scheidet demnach aus.[553]

Die Datenverarbeitung darf grundsätzlich gem. § 14 Abs. 1 BDSG nur zu dem Zweck stattfinden, zu dem die Daten zuvor auch erhoben worden sind. Die gesetzliche Aufgabenzuweisungsnorm muss demnach nicht nur die Erhebung der Daten erfordern sondern auch ihre weitergehende Verarbeitung. Sollen die einmal erhobenen Daten für andere Zwecke weiterverarbeitet werden, so muss eine der abschließend in § 14 Abs. 2 BDSG aufgezählten Ausnahmen eingreifen.[554] Die Vorschriften für die Datenübermittlung verweisen hinsichtlich der weitergehenden Zulässigkeitsvoraussetzungen auf § 14 BDSG. Die Übermittlung an nicht-öffentliche Stellen ist ausnahmsweise auch dann zulässig, wenn die empfangende Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Damit bleibt festzuhalten, dass die Legitimierung der Datenverarbeitung durch öffentliche Stellen nur bei Einhaltung der sich unmittelbar aus dem Gesetz ergebenden Voraussetzungen möglich ist. Lediglich bei Überschneidungen mit dem nicht-öffentlichen Bereich (§ 16 BDSG) kann auch auf die Interessen der empfangenden Stelle abgestellt werden, was eine nicht zu unterschätzende Erweiterung der Legitimierungsmöglichkeiten darstellt. Diese Abwägung der Interessen der datenverarbeitenden Stelle mit den Interessen des Betroffenen ist hingegen Charakteristikum der Datenverarbeitung durch nicht-öffentliche Stellen (s. sogleich unten).

---

[552] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 13 Rn. 9.

[553] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 13 Rn. 15.

[554] Vgl. zu den einzelnen Ausnahmetatbeständen *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 14 Rn. 13 ff.

bb) Rechte des Betroffenen, §§ 19 ff. BDSG

In §§ 19 bis 21 BDSG finden sich die Rechte des Betroffenen bei der Verarbeitung seiner Daten durch öffentliche Stellen. Namentlich sind dies das Recht auf Auskunft (§ 19), Benachrichtigung (§ 19a), Berichtigung, Löschung und Sperrung sowie Widerspruch (§ 20) und zuletzt das Recht auf Anrufung des Bundesdatenschutzbeauftragten für die Fälle einer behaupteten Rechtsverletzung (§ 21).

Das Auskunftsrecht bildet hierbei die Basis für alle weiteren Rechte, denn – so bereits das Bundesverfassungsgericht[555] – nur wer weiß, wer wann wie und in welchem Umfang seine personenbezogenen Daten erhebt und verarbeitet kann auch von seinen gesetzlich garantierten Rechten Gebrauch machen.

cc) Leading Scenarios

Szenario 1

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

Auf die Rechtmäßigkeit der Verarbeitung der auf den von den Meldebehörden ausgegebenen Ausweispapieren gespeicherten Daten soll hier nicht weiter eingegangen werden. Solche Verarbeitungen richten sich nach den einschlägigen Spezialgesetzen – PassG sowie PAuswG.

Die Ausgabe sonstiger RFID-Tags i.S.v. Szenario 1 durch öffentliche Stellen ist denkbar und auch geplant. Die Bundesregierung hat bereits 2006 angekündigt, dass geplant sei „die in der Bundesverwaltung eingesetzten, unterschiedlich gestalteten Dienstausweise durch einen einheitlichen digitalen Dienstausweis in Form einer multifunktionalen Chipkarte zu ersetzen“.[556]

Sofern eine solche Ausgabe stattfindet, müssen sich die damit verbundenen Datenverarbeitungsmaßnahmen seitens der öffentlichen Stelle an den strengen Maßstäben der §§ 13 ff. BDSG messen lassen und diese vornehmlich zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich sein.

Szenario 2

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

Ein relevanter Anwendungsfall i.S.v. Szenario 2 wäre gegeben, wenn in deutschen Justizvollzugsanstalten dauerhaft mit dem Körper der Insassen verbundene RFID-Tags – Fußfesseln

[555] BVerfGE 65, 1 (43) – Volkszählung.

[556] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Rainer Brüderle, Ernst Burgbacher, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/3025 – Technologie der Radio Frequency Identification, BTDrucks. 15/3190 vom 26. 05. 2004 abrufbar unter http://dipbt.bundestag.de/dip21/btd/15/031/1503190.pdf (04.04.2013), S. 4.

o.ä. wie in US-amerikanischen Gefängnissen teilweise schon eingesetzt – verwendet würden. Im Rahmen des Strafvollzugs wären solche Maßnahmen aber wohl relativ unproblematisch gerechtfertigt. Insbesondere ist nicht ersichtlich, wie die Überwachung der Insassen mittels RFID weitergehend in deren Persönlichkeitsrecht eingreifen würde, als dies bereits heute mittels konventioneller Kontrollmechanismen der Fall ist. Die Datenverarbeitung innerhalb des Strafvollzuges richtet sich nach dem StVollzG, das in Titel 5 (§§ 179 ff.) spezielle Regelungen für den Datenschutz bereithält.

Szenario 3

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

Eine Anwendung i.S.v. Szenario 3 sind an die im öffentlichen Dienst ausgegebenen RFID-Tokens, die als Türöffner, Kantinenkarte u.ä. genutzt werden können. In diesem Fall ist auf dem Tag selbst nur die Identifikationsnummer gespeichert. Im Hintergrundsystem hingegen muss eine Zuordnung zur Person des Tag-Inhabers vorgenommen werden können und mithin weitergehende Daten gespeichert sein. Die Erhebung und weitergehende Nutzung der Tag-Daten hat sich nach den Vorgaben der §§ 13 ff. BDSG zu richten. Die Erhebung der Tag-Daten in verschiedenen Situationen ist nach § 13 Abs. 1 BDSG nur dann gerechtfertigt, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Bei der Verwendung als Türöffner wäre dies die Kontrolle, ob der Betroffene berechtigt zum Betreten der nicht-öffentlichen Räumlichkeiten ist, beim Zahlen in der Kantine die Abrechnung mit dem Kantinenkonto des Betroffenen. Die weitergehende Verwendung der erhobenen Daten ist gem. § 14 Abs. 1 BDSG grundsätzlich nur erlaubt, soweit diese ebenfalls für die Aufgabenerfüllung der öffentlichen Stelle erforderlich ist. Eine Speicherung der im Rahmen der Zutrittskontrolle anfallenden Daten ist vor diesem Hintergrund kaum zu rechtfertigen, entfällt doch der Zweck – Überprüfung der Autorisation des Betroffenen zum Betreten der Räume – in dem Moment des Abgleichs. Auch die bei einem Bezahlvorgang erhobenen Daten – also insbesondere Zeit- und Ortsangabe – dürfen nicht gespeichert werden, sind sie doch für die Abrechnung mit dem Betroffenen nicht erforderlich. Eine Rechtfertigung käme dann regelmäßig nur noch mittels Einwilligung des Betroffenen in Betracht, § 14 Abs. 2 Nr. 2 BDSG. Im Einzelfall wäre natürlich zu prüfen, ob auch eine andere Ausnahme eingreift.

Szenario 4

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur weiterführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

Eine Ausgabe von Tags i.S.v. Szenario 4 durch öffentliche Stellen erscheint ebenfalls denkbar. In einer ubiquitären RFID-Umgebung wären auch alle im öffentlichen Dienst verwende-

ten Materialien getaggt. Indes käme es dann darauf an, ob die öffentliche Stelle auch die weitere RFID-Infrastruktur, namentlich kompatible Lesegeräte, einsetzte. Sofern lediglich Lesegeräte zum Erfassen solcher RFID-Tags i.S.v. Szenario 3 eingesetzt würden, die nicht dazu genutzt würden auch produktbezogene Tags zu lesen und damit gegebenenfalls Bewegungsprofile zu erstellen, stellt sich auch nicht das Bedürfnis nach einer datenschutzrechtlichen Rechtfertigung. Dass ein solches Vorgehen von Behörden geplant wäre, ist zum jetzigen Zeitpunkt nicht bekannt.

e) Besondere Regelungen für die Datenverarbeitungen nicht-öffentlicher Stellen

Die besonderen Regelungen für die Datenverarbeitungen nicht-öffentlicher Stellen – Erlaubnistatbestände sowie die Vorschriften über die Betroffenenrechte – finden sich in §§ 28 ff. und §§ 33 ff. BDSG. Anders als bei der Datenverarbeitung durch öffentliche Stellen kommt es bei der Datenverarbeitung durch nicht-öffentliche Stellen, zu denen gem. § 27 Abs. 1 S. 2 Nr. 2 BDSG auch öffentlich-rechtliche Wettbewerbsunternehmen gehören, in vielen Fällen auf eine Abwägung der sich gegenüberstehenden Interessen der datenverarbeitenden Stelle und des Betroffenen an.

aa) Erlaubnistatbestände für die Datenverarbeitung

Die in den §§ 28 ff. BDSG enthaltenen Erlaubnistatbestände für die Datenverarbeitung nicht-öffentlicher Stellen beinhalten eine Reihe unbestimmter Rechtsbegriffe, so beispielsweise den Begriff der „Zweckbestimmung des Vertragsverhältnisses“, die „berechtigten Interessen“ der verantwortlichen Stelle oder das „überwiegende schutzwürdige Interesse des Betroffenen“. Die Erforderlichkeit der Auslegung dieser Rechtsbegriffe kann dazu genutzt werden, den Anwendungsbereich des entsprechenden Erlaubnistatbestandes zugunsten der verarbeitenden Stelle auszuweiten.[557] Hierin liegt ein entscheidender Unterschied zu den Regelungen über die Datenverarbeitung durch öffentliche Stellen. Entsprechend ist bei der Auslegung dieser Begriffe besonderes Augenmerk auf die potenzielle Gefährdung des Persönlichkeitsrechts des Betroffenen in der konkreten Anwendung zu richten.

Im Rahmen von RFID-Anwendungen werden maßgeblich § 28 BDSG und die dort geregelten Erlaubnistatbestände heranzuziehen sein. Die Vorschriften über die Datenübermittlung an Auskunfteien (§ 28a BDSG), Scoring (§ 28b BDSG), die geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung (§ 29 BDSG) sowie die geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form (§ 30 BDSG) dürften regelmäßig nicht einschlägig sein, sodass auf eine Darstellung selbiger in dieser Arbeit verzichtet wird. Relevanz könnte hingegen § 30a BDSG über die geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung zukommen. Insbesondere bei der massenhaften Erstellung von Kundenprofilen bzw. der Analyse von Kundenverhalten o.ä.[558] findet die Vorschrift gegebenenfalls Anwendung.

---

[557] *Simitis* in: Simitis, BDSG, § 28 Rn. 21.

[558] S.o. C.II.2.

aaa) Erfüllung eigener Geschäftszwecke, § 28 BDSG

§ 28 Abs. 1 BDSG regelt die Verarbeitung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke und ist der wichtigste Anwendungsfall des § 28. Für andere als eigene Geschäftszwecke dürfen personenbezogene Daten nur unter den jeweiligen Voraussetzungen der Absätze 2 bis 5 erfolgen. Besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) dürfen für eigene oder sonstige Zwecke unter den Voraussetzungen der Absätze 6 bis 9 verarbeitet werden.

Eine Datenverarbeitung im Rahmen eigener Geschäftszwecke ist dann anzunehmen, wenn die datenverarbeitende Stelle – in Abgrenzung zu § 29 BDSG – ein eigenes Interesse an der Datenverarbeitung hat, diese aber nur Mittel zum Zweck der Erfüllung des eigentlichen Geschäftszwecks ist.[559] Die Erhebung zum ausschließlichen Zwecke der Monetisierung der Daten – Verkauf und Weitergabe – führt entsprechend zu einer Anwendung von § 29 BDSG.

Erste Stufe in der Reihe der denkbaren Datenverarbeitungsmaßnahmen (§ 3 Abs. 4 BDSG) ist die Erhebung der Daten (§ 3 Abs. 3 BDSG). Zwar hat der Gesetzgeber der Erhebung eine Sonderstellung eingeräumt, er sieht sie aber dennoch als Grundlage für alle weiteren Verarbeitungsschritte. Dies wird besonders deutlich aus der Formulierung des Zweckbindungsgrundsatzes, § 28 Abs. 1 S. 2 BDSG. Die Zwecke der Erhebung sowie der weitergehenden Verarbeitung sind vorab – also bereits vor der Erhebung – durch die datenverarbeitende Stelle festzulegen.

§ 28 Abs. 1 S. 1 BDSG unterscheidet drei verschiedene Erlaubnistatbestände. Die Datenverarbeitung ist hiernach gerechtfertigt,

(1) wenn sie für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (Nr. 1),
(2) soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (N. 2) oder
(3) wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt (Nr. 3).

Dem Gesetzeswortlaut nach stehen die drei selbstständigen Tatbestände in einem Alternativverhältnis. Hierbei ist jedoch zu berücksichtigen, dass der Gesetzgeber davon ausging, dass Datenverarbeitungen im Rahmen eines Schuldverhältnisses der Regelfall sein sollen; der Rückgriff auf die berechtigten Interessen (Nr. 2) sowie die allgemein zugänglichen Daten (Nr. 3) soll grundsätzlich nur nachrangig dann erfolgen, wenn ein Schuldverhältnis zwischen den Parteien nicht vorliegt.[560] Folglich steht es auch nicht im Belieben der datenverarbeiten-

[559] *Simitis* in: Simitis, BDSG, § 28 Rn. 22.

[560] *Gola/Schomerus*, BDSG, § 28 Rn. 9.

den Stelle, welche Alternative zur Rechtfertigung der konkreten Datenverarbeitungsmaßnahme sie wählt oder gar nach eigenem Gusto ergänzend auf mehrere Erlaubnistatbestände zurückzugreifen.[561]

Vorrangig ist also immer zu überprüfen, ob ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis zwischen Betroffenem und datenverarbeitender Stelle vorliegt, zu dessen Begründung, Durchführung oder Beendigung die Verarbeitung der in Frage stehenden personenbezogenen Daten erforderlich ist. Hinsichtlich des Begriffs des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses kann auf das bürgerliche Recht verwiesen werden. Gemeinhin wird es sich um einen Vertrag oder aber eine Vertragsanbahnung zwischen den Parteien handeln.[562] Der in § 28 Abs. 1 S. 1 Nr. 1 BDSG formulierte Erforderlichkeitsgrundsatz bewirkt, dass die Verarbeitung der in Frage stehenden personenbezogenen Daten für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich sein muss, dass sie also zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus einem mit dem Betroffenen geschlossenen Vertrag vorgenommen werden muss.[563] § 28 Abs. 1 S. 1 Nr. 1 BDSG setzt damit jedenfalls einen unmittelbaren sachlichen Zusammenhang zwischen der beabsichtigten Verarbeitung und dem konkreten Vertragszweck voraus[564], er darf indes wohl nicht dahingehend interpretiert werden, dass der Geschäftszweck überhaupt nicht auf andere Weise erreicht werden können darf, weil solche Sachverhalte außerordentlich selten wären[565].

Der Zweck des Schuldverhältnisses kann sich unmittelbar aus dem Vertragswortlaut oder aber durch Auslegung der jeweiligen Rechte und Pflichten der Parteien ergeben.[566] Nicht vom Vertragszweck umfasst ist regelmäßig die Nutzung erhobener Kundendaten zu Werbezwecken. Sollen Im Rahmen eines Schuldverhältnisses erhobene Daten auch zu Werbezwecken eingesetzt werden, so sind die besonderen Bestimmungen in § 28 Abs. 3 ff. BDSG zu berücksichtigen; ohne Einwilligung ist Werbung anhand solcher Daten unzulässig, es sei denn, es handelt sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer bestimmten Personengruppe.[567] Bei der Erfassung von Bewegungsdaten der eigenen Kunden ist im Einzelfall zu prüfen, ob solche Daten für die Erfüllung des zu Grunde liegenden Vertrags erforderlich sind.[568]

Soweit die Datenverarbeitung nicht durch das bestehende oder infolge des Fehlens eines Schuldverhältnisses nicht gedeckt ist, kommt eine Rechtfertigung gem. § 28 Abs. 1 S. 1 Nr. 2

---

[561] *Simitis* in: Simitis, BDSG, § 28 Rn. 77.

[562] Vgl. zu den Einzelheiten *Gola/Schomerus*, BDSG, § 28 Rn. 12 f.

[563] *Gola/Schomerus*, BDSG, § 28 Rn. 15.

[564] *Simitis* in: Simitis, BDSG, § 28 Rn. 79.

[565] *Gola/Schomerus*, BDSG, § 28 Rn. 15; a.A. *Wedde* in: Däubler/Klebe/Wedde/Weichert, BDSG § 28 Rn. 15.

[566] *Gola/Schomerus*, BDSG, § 28 Rn. 17.

[567] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 41.

[568] Nicht erforderlich ist diese Art der Profilierung z.B. im Rahmen eines Vertrags zwischen Betroffenem und Fitnessstudiobetreiber, vgl. *Simitis* in: Simitis, BDSG, § 28 Rn. 91.

BDSG wegen überwiegender berechtigter Interessen der datenverarbeitenden Stelle in Betracht. Hierbei ist zu berücksichtigen, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG nicht als Auffangtatbestand gedacht ist.[569] Entsprechend kann die datenverarbeitende Stelle nicht ohne weiteres auf ihn zurückgreifen, sofern die Datenverarbeitungsmaßnahme nicht bereits vor dem Hintergrund eines bestehenden Schuldverhältnisses gerechtfertigt ist.[570] Insbesondere die Verarbeitung in einem über den zur Erreichung des vertraglichen Zwecks erforderlichen Umfangs hinaus, kann nicht ohne weiteres durch sonstige Interessen der datenverarbeitenden Stelle gerechtfertigt werden.[571] Zwar kann grundsätzlich jedes eigene von der Rechtsordnung gebilligte Interesse der datenverarbeitenden Stelle ein berechtigtes Interesse sein[572], allerdings ist zu fordern, dass dieses mit der konkret beabsichtigten Datenverarbeitung zusammenhängt und sich auf Daten bezieht, die dabei verwendet werden sollen.[573] Ein berechtigtes Interesse der datenverarbeitenden Stelle kann grundsätzlich bei Maßnahmen zur personalisierten Werbung bestehen; die Bindung der Kunden an das eigene Geschäft sowie verstärkte Bemühungen, den bestehenden Kundenkreis zu erweitern, sind legitime geschäftspolitische Ziele.[574] Indes ist insbesondere in diesem Fall bei Vorliegen eines Vertragsverhältnisses i.S.v. § 28 Abs. 1 S. 1 Nr. 1 BDSG darauf zu achten, dass der Erlaubnistatbestand nach Nr. 2 dazu herangezogen wird, ein Verhalten zu legitimieren, welches nach dem Vertragszweck illegitim wäre (s. schon oben). Im Zweifel sind die erweiterten Voraussetzungen des § 28 Abs. 3 BDSG zu berücksichtigen.

Die in Frage stehende Datenverarbeitung muss wiederum zur Wahrung dieses berechtigten Interesses erforderlich sein.[575] Nicht erforderlich ist grundsätzlich die Erstellung umfassender Kundenprofile „auf Halde“ beispielsweise in Form von *Data Warehouses*[576]; dies verbietet sich vor dem Hintergrund des informationellen Selbstbestimmungsrechts, weil bei pauschaler und fortwährender Datenerhebung und -speicherung der Betroffene keinen Überblick mehr über die gesammelten Daten hat.[577]

Ausgeschlossen ist die Rechtfertigung gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG, sofern Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffen am Ausschluss der Datenverarbeitung überwiegen. Bei der Bewertung etwaiger Interessen des Betroffenen ist u.a. auf die mit der Verarbeitung zu befürchtenden wirtschaftlichen oder beruflichen Nachteile abzustellen.[578] Sofern schutzwürdige Interessen auf Seiten des Betroffenen zu bejahen sind, ist im

---

[569] *Simitis* in: Simitis, BDSG, § 28 Rn. 134.

[570] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 47.

[571] *Simitis* in: Simitis, BDSG, § 28 Rn. 134.

[572] *Gola/Schomerus*, BDSG, § 28 Rn. 24; Taeger/Gabel/*Taeger*, § 28 BDSG, Rn. 55.

[573] *Simitis* in: Simitis, BDSG, § 28 Rn. 137.

[574] *Simitis* in: Simitis, BDSG, § 28 Rn. 159.

[575] *Gola/Schomerus*, BDSG, § 28 Rn. 25.

[576] Taeger/Gabel/*Taeger*, § 28 BDSG, Rn. 57.

[577] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 55.

[578] *Gola/Schomerus*, BDSG, § 28 Rn. 26.

Folgenden eine Interessenabwägung im Einzelfall vorzunehmen. Der BGH hat hierzu einen Leitfaden ausgegeben:

> „Der wertausfüllende Begriff der „schutzwürdigen" Belange verlangt eine Abwägung des Persönlichkeitsrechts des Betroffenen und des Stellenwerts, den die Offenlegung und Verwendung der Daten für ihn hat, gegen die Interessen der speichernden Stelle und der Dritten, für deren Zweck die Speicherung erfolgt. Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Angaben und Zwecken zu messen, denen ihre Speicherung dient. Nur wenn diese am Verhältnismäßigkeitsgrundsatz ausgerichtete Abwägung, die die speichernde Stelle vorzunehmen hat, keinen Grund zur Annahme bietet, dass die Speicherung der in Frage stehenden Daten zu dem damit verfolgten Zweck schutzwürdige Belange des Betroffenen beeinträchtigt, ist die Speicherung zulässig."[579]

Da darauf abzustellen ist, ob Grund zu der *Annahme* besteht, dass schutzwürdige Belange des Betroffenen überwiegen, kommt es nicht auf solche Umstände an, die für die datenverarbeitende Stelle nicht erkennbar sind.[580] Sie muss entsprechend nicht jede theoretisch denkbare Annahme einer möglichen Interessenverletzung berücksichtigen, sondern lediglich die Umstände, die für sie erkennbar sind.[581] Gleichzeitig kommt es auf einen tatsächlich entgegenstehenden Willen des Betroffenen nicht notwendigerweise an, sofern sich infolge der Interessenabwägung ergibt, dass seine Interessen nicht überwiegen, allerdings muss ein solcher in besonderem Maße bei der Interessenabwägung Berücksichtigung finden.[582]

Die letzte Alternative zur Rechtfertigung etwaiger Datenverarbeitungen gem. § 28 Abs. 1 S. 1 Nr. 3 BDSG erlaubt diese bei allgemein zugänglichen Daten oder solchen Daten, die von der datenverarbeitenden Stelle veröffentlicht werden dürften. Auch bei Nr. 3 muss eine Interessenabwägung vorgenommen werden, bei der allerdings lediglich ein offensichtliches Überwiegen schutzwürdiger Betroffeneninteressen zu einem Wegfall der Legitimation der Datenverarbeitung führt. Öffentlich zugängliche Quellen i.S.d Norm sind hierbei nur solche, „die sich sowohl ihrer technischen Ausgestaltung als auch ihrer Zielsetzung nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln"[583].

Die Datenverarbeitung für andere als die in § 28 Abs. 1 BDSG genannten Zwecke ist nur unter den zusätzlichen Voraussetzungen der Abs. 2 bis 5 erlaubt. Speziell für die Verarbeitung zu Werbezwecken, welche wie oben gezeigt insbesondere bei RFID-Anwendungen im Einzelhandel künftig eine wichtige Rolle spielen dürften, stellt § 28 Abs. 3 bis 5 BDSG spezielle Anforderungen auf. Wichtigstes Merkmal ist, dass – soweit es sich nicht um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt – immer die Einwilligung des Betroffenen in die Verwendung seiner Daten zu Werbezwecken einzuholen ist. D.h., dass bei allen individuell erhobenen Datensätzen – in Abgrenzung zu Listen mit Angaben über mehr als eine Person[584] – durch die datenverarbeitende Stelle selbst auch immer

---

[579] BGH NJW 1986, 2505 (2506).

[580] *Gola/Schomerus*, BDSG, § 28 Rn. 28.

[581] *Gola/Schomerus*, BDSG, § 28 Rn. 28.

[582] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 53; im Ergebnis auch *Simitis* in: Simitis, BDSG, § 28 Rn. 180, 181.

[583] *Simitis* in: Simitis, BDSG, § 28 Rn. 189 m.w.N.

[584] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 97.

die Einwilligung seitens des Betroffenen erfolgen muss. Diese kann zwar gem. § 28 Abs. 3a BDSG auch in anderer als der schriftlichen Form erteilt werden, die datenverarbeitende Stelle muss sie zu Beweiszwecken allerdings in geeigneter Form dokumentieren.[585]

bbb) Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung, § 30a BDSG

§ 30a BDSG ist eine mit der BDSG-Novelle von 2009 neu eingefügte Vorschrift, die den Besonderheiten der Markt- und Meinungsforschung und dem hiermit im Zusammenhang stehenden Bedarf an der Erhebung personenbezogener Daten unter erleichterten Bedingungen – insbesondere unter Verzicht auf das Einwilligungserfordernis[586] – Rechnung tragen soll.[587] Maßnahmen der Markt- und Meinungsforschung sind hierbei von solchen der Werbung abzugrenzen. Für letztere gilt weiterhin vornehmlich § 28 BDSG. Als Unterscheidungsmerkmal soll es hierbei darauf ankommen, dass die Datenverarbeitung geschäftsmäßig, also nicht nur einmalig und insbesondere für spätere Werbeansprachen[588], von der datenverarbeitenden Stelle vorgenommen wird, vielmehr muss der Analysecharakter im Vordergrund stehen.[589] Adressat der Vorschrift sind indes nicht nur Meinungsforschungsinstitute u.ä. sondern alle Unternehmen, die Markt- und/oder Meinungsforschung betreiben – und zwar sowohl für fremde als auch für eigene Zwecke.[590] Die Anwendung von § 30a BDSG auf massenhafte RFID-gestützte Datenerhebungen und -analysen – wie insbesondere im Einzelhandelsbereich erwartet – ist dennoch abzulehnen. Bei den oben dargestellten Verfahren des Tracking und Profiling (C.II) handelt es sich um Markt- und Meinungsforschungen, die ein Unternehmen lediglich zu eigenen Zwecken wie der Förderung von Kundenbeziehungen – auch mittels Schaltung personalisierter Werbung – durchführt. Diese fallen als Werbemaßnahmen unter § 28 BDSG.[591] Auch wenn das eigene Geschäft maßgeblich von solchen Verfahren profitieren kann, wird damit doch noch nicht die Geschäftsmäßigkeit der Markt- und Meinungsforschungstätigkeit begründet. Diese wird vielmehr als Mittel zum Zweck eingesetzt werden. § 30a BDSG wird damit jedenfalls in den benannten RFID-Anwendungen nicht anwendbar sein.

bb) Informationspflichten, § 33 BDSG

§ 33 BDSG statuiert in Ergänzung zu § 4 Abs. 3 BDSG Informationspflichten der datenverarbeitenden Stelle gegenüber dem Betroffenen. Während § 4 Abs. 3 BDSG die Pflicht zur Information bei der Datenerhebung aufstellt, bezieht sich § 33 BDSG auf alle weitergehenden Datenverarbeitungsmaßnahmen. § 33 BDSG bezieht sich hierbei nur auf Datenverarbeitungsmaßnahmen, die zum ersten Mal und ohne Kenntnis des Betroffenen stattfinden. Hiermit

---

[585] *Wedde* in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 93.

[586] Taeger/Gabel/*Munz*, § 30a BDSG, Rn. 6.

[587] Taeger/Gabel/*Munz*, § 30a BDSG, Rn. 15.

[588] *Weichert* in: Däubler/Klebe/Wedde/Weichert, § 30a Rn. 2.

[589] Taeger/Gabel/*Munz*, § 30a BDSG, Rn. 10; *Gola/Schomerus*, BDSG, § 30a Rn. 1.

[590] Taeger/Gabel/*Munz*, § 30a BDSG, Rn. 10, 11.

[591] *Gola/Schomerus*, BDSG, § 30a Rn. 1.

korreliert auch der Ausnahmetatbestand zur Benachrichtigungspflicht für die Fälle, in denen der Betroffene schon auf anderem Wege von der Verarbeitung Kenntnis erlangt hat, § 33 Abs. 2 S. 1 Nr. 1 BDSG. Die Informationspflicht entfällt indes nicht bereits dann, wenn der Betroffene zwar von der Datenverarbeitungsmaßnahme als solcher, nicht aber all ihren näheren Umständen wie in § 33 Abs. 1 BDSG aufgezählt, Kenntnis erlangt hat; nur ein voll informierter Betroffener muss demnach nicht mehr informiert werden.[592] Dementsprechend entsteht eine wiederholte Benachrichtigungspflicht auch immer dann, wenn sich die Art der zu speichernden Daten oder aber die Zweckbestimmung der Verarbeitung ändert; in diesen Fällen ist der Betroffene nämlich gerade nicht mehr umfassend informiert.[593] Hinsichtlich der Form der Benachrichtigung gilt, dass der Betroffene individuell informiert werden muss, sodass regelmäßig Hinweise in allgemeinen Geschäftsbedingungen nicht ausreichen, jedenfalls so lange nicht, wie der Betroffene diese nicht eingesehen hat.[594]

cc) Rechte des Betroffenen, §§ 34, 35 BDSG

Die in §§ 34 und 35 BDSG geregelten Betroffenenrechte umfassen einerseits das Recht auf Auskunft und andererseits die Pflicht zur Berichtigung, Löschung und Sperrung von Daten, sofern die Voraussetzungen für die Verarbeitung nicht mehr gegeben sind. Beide Rechte sind unabdingbar, § 6 Abs. 1 BDSG. Das Auskunftsrecht ist hierbei die Grundlage weiterer Rechteausübungen: Ohne Kenntnis, welche Daten die verantwortliche Stelle vom Betroffenen gespeichert hat und verarbeitet, kann dieser auch nicht von einem etwaigen Recht auf Löschung oder Berichtigung Gebrauch machen. Auskunft ist dem Betroffenen auf dessen Antrag regelmäßig kostenlos über alle bei der verantwortlichen Stelle gespeicherten personenbezogenen Daten über den Betroffenen zu erteilen.[595]

Die weitergehenden Pflichten der verantwortlichen Stelle ergeben sich grundsätzlich bereits aus dem Gesetz, sprich, es kommt nicht darauf an, dass der Betroffene die verantwortliche Stelle zur Vornahme der gebotenen Handlung auffordert. Allerdings kann die Aufforderung des Betroffenen bzw. ein entsprechender Antrag die Kenntnisnahme der verantwortlichen Stelle bewirken, wodurch die Handlungspflicht begründet wird.[596] Weiterhin räumt § 35 Abs. 5 BDSG dem Betroffenen ein Widerspruchsrecht für die Fälle ein, in denen die Datenverarbeitung wegen vorrangiger öffentlicher oder privater Interessen gestattet wird. Der Betroffene kann dann sich aus seiner persönlichen Situation ergebende Gründe vortragen, die den Interessen der datenverarbeitenden Stelle vorrangig sind.[597] Ergibt sich nach einer entsprechenden Prüfung und Abwägung, dass der Widerspruch berechtigt ist, muss die entsprechende Datenverarbeitung unterbleiben.

---

[592] *Gola/Schomerus*, BDSG, § 33 Rn. 6.

[593] *Gola/Schomerus*, BDSG, § 33 Rn. 16.

[594] *Gola/Schomerus*, BDSG, § 33 Rn. 18.

[595] *Gola/Schomerus*, BDSG, § 34 Rn. 4 ff., 9 ff., 20 ff.

[596] Vgl. *Gola/Schomerus*, BDSG, § 35 Rn. 3.

[597] *Gola/Schomerus*, BDSG, § 35 Rn. 28.

dd) Leading Scenarios

Für die herausgearbeiteten *Leading Scenarios* ergibt sich nach obigen Ausführungen folgendes:

Szenario 1

(1) RTAMP – Extrinsic Ubiquity:

Auf dem RFID-Tag sind personenbezogene Daten wie Name, Anschrift, Iris-Scan, Fingerabdruck etc. gespeichert (z.B. RFID-Tag im neuen Pass oder Personalausweis sowie in einigen ÖPNV-Tickets).

Hinsichtlich der Daten, die auf den Tags in Ausweispapieren gespeichert sind, und ihrer Verarbeitung gilt weiterhin, dass als Rechtfertigungsgründe die Normen der einschlägigen Gesetze heranzuziehen sind. Diese werden ohnehin von öffentlichen Stellen ausgegeben. Aber auch die Verarbeitung der auf den Tags gespeicherten Daten durch nicht-öffentliche Stellen – wie es in einem gewissen Rahmen gestattet ist – richtet sich aufgrund des abschließenden Charakters nach diesen Gesetzen, sodass auch hierauf an dieser Stelle nicht weiter eingegangen werden soll.

Bei sonstigen Tags, die in der Privatwirtschaft eingesetzt werden, wie beispielsweise ÖPNV-Tickets, ist zunächst im Rahmen der Rechtfertigung gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG jeweils das zugrunde liegende Vertragsverhältnis zu betrachten: Ist die Erreichung des vertraglichen Zwecks auf die Verarbeitung der betreffenden personenbezogenen Daten erforderlich, oder nicht? Hierbei gilt bereits oben beim Grundsatz der Datenvermeidung und Datensparsamkeit Gesagtes: Unterschiedliche Einschätzungen der Erforderlichkeit können sich bei unterschiedlichen Tickets – übertragbare oder nicht- übertragbare – ergeben. Nur bei Tickets, bei denen die verantwortliche Stelle ein Recht darauf hat, die Identität des jeweiligen Fahrgastes vor Ort zu überprüfen, ist die Speicherung personenbezogener Daten auf dem Tag vom Vertragszweck umfasst. Ist das Ticket hingegen übertragbar, so genügt die Feststellung, ob das Ticket gültig ist oder nicht. Hierfür bedarf es nicht einmal der Speicherung einer eindeutigen Identifikationsnummer. Vielmehr genügen in diesen Fällen Tags vergleichbar mit solchen, die zur elektronischen Diebstahlsicherung verwendet werden. Das Tag muss lediglich in der Lage sein zwei Zustände kenntlich zu machen, nämlich gültig – der (anonyme) Fahrgast ist berechtigt mit dem Verkehrsmittel zu fahren – oder nicht gültig – der Fahrgast fährt schwarz.

Für weitergehende Zwecke dürfen Tags mit personenbezogenen Daten allerdings verwendet werden, sofern dies ausdrücklich als Zielbestimmung in den Vertrag mit aufgenommen worden ist. Die Anfertigung personalisierter Bewegungsmuster zum Beispiel zwecks Fahrplanoptimierung oder ähnlichem kann entsprechend gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG gerechtfertigt sein, wenn dies Gegenstand des Vertrags ist.

Ist eine über den bloßen Transport mittels ÖPNV hinausgehende Zweckbestimmung nicht Vertragsgegenstand, so ist eine weitergehende Datenverarbeitung auch nicht gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG zu rechtfertigen. Inwieweit dann eine Rechtfertigung wegen überwiegender berechtigter Interessen der verantwortlichen Stelle gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG in Be-

tracht kommt, hängt maßgeblich davon ab, inwieweit bereits eine Sperrwirkung durch das Vorliegen eines Vertragsverhältnisses zu bejahen ist. Ein Interesse an der Erstellung personalisierter Bewegungsprofile kann sich z.B. aus Geschäftsoptimierungsgründen wie oben dargestellt ergeben. Auch der Wille zur Unterstützung der Polizei bei der Aufklärung von Straftaten – wie in London bei der Oyster Card geschehen[598] – kann ein Interesse der verantwortlichen Stelle an der fortwährenden Ortung der Fahrgäste begründen. Problematisch stellt sich die Grenzziehung dar: Welches Interesse ist unter Berücksichtigung des Vertrags und des mit diesem verfolgten Zwecks noch als berechtigtes anzusehen? Infolge des Erfordernisses einer restriktiven Auslegung muss genau geprüft werden, ob ein berechtigtes Interesse der verantwortlichen Stelle tatsächlich gegeben ist. Eine Grenze kann wohl da gezogen werden, wo ein Unternehmen ein allgemeines Interesse daran geltend macht, RFID-Tags pauschal auszulesen ohne beim Erhebungsvorgang bereits den konkreten späteren Verwendungszweck – z.B. Anlegung von Profilen oder Aufklärung von Straftaten – festgelegt zu haben.[599] Das Erheben und Speichern „auf Halde“ in jeder Form und in jedem Umfang kann nicht über § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigt werden. Sofern indes von vornherein feststeht, dass die Daten zur Erstellung von Bewegungsprofilen zwecks Geschäftsoptimierung genutzt werden sollen, dürfte in der Tat ein berechtigtes – nämlich wirtschaftliches – Interesse der verantwortlichen Stelle zu bejahen sein.

Erlaubt wäre die Datenerhebung im Einzelfall indes nur, wenn nicht überwiegende schutzwürdige Interessen des Betroffenen vorliegen. Pauschal davon auszugehen, dass kein Fahrgast berechtigte Interessen gegen eine solche Profilierung wird eizuwenden haben, wäre verfehlt. Gleichfalls werden auch nicht alle Fahrgäste sich an solchen Profilierungen stören. Dem Wortlaut des Gesetzes nach muss die verantwortliche Stelle überprüfen, ob Grund zu der Annahme besteht, dass überwiegende schutzwürdige Interessen beim Betroffenen vorliegen. Dieser Grund zur Annahme kann sich der verantwortlichen Stelle aufdrängen, wenn der Betroffene der Datenverarbeitung widersprochen hat. Geschieht dies nicht, muss die verantwortliche Stelle auf der anderen Seite nach vielfach vertretener Meinung aber auch nicht nachfragen.[600] Gerade vor dem Hintergrund der Möglichkeit andauernder Überwachung und Profilierung des Betroffenen stellt sich aber die Frage, ob man die verantwortliche Stelle so einfach aus ihrer Verantwortung entlassen kann. Nicht vergessen werden darf das vom Bundesverfassungsgericht herausgearbeitete Recht auf informationelle Selbstbestimmung, welches gerade den grundsätzlichen Anspruch des Einzelnen verbürgt, nicht dauernd überwacht zu werden. Ließe man nunmehr auf einfachgesetzlicher Ebene zu, dass Unternehmen, die zur Überwachung geeignete Techniken einsetzen wollen, *in der Regel* davon ausgehen dürfen, dass keine entgegenstehenden Interessen beim Betroffenen vorliegen, konterkarierte man den Wertgehalt, den das Bundesverfassungsgericht dem Recht auf informationelle Selbstbestimmung beimisst. Insofern gilt es einen Kompromiss zwischen dem grundsätzlichen Ausschluss einer Nachforschungspflicht seitens der verantwortlichen Stelle und dem Wertgehalt des Rechts auf

[598] Vgl. oben C.II.1.

[599] Taeger/Gabel/*Taeger*, § 28 BDSG, Rn. 57.

[600] Vgl. nur bei Taeger/Gabel/*Taeger*, § 28 BDSG, Rn. 63; *Simitis* in: Simitis, BDSG, § 28 Rn. 165.

informationelle Selbstbestimmung andererseits zu finden. Mangels klaren Prüfungsschemas, welches die verantwortliche Stelle anzuwenden hätte, kann lediglich gefordert werden, dass diese die Verarbeitungsfolgen für die im *Einzelfall* betroffenen Personen prüft.[601] Eine solche Einzelfallprüfung erscheint in einer mittels ubiquitärer RFID-Infrastruktur durchzuführenden Massendatenverarbeitung mit unabsehbar vielen Betroffenen faktisch ausgeschlossen. Dies wiederum führt nicht automatisch zu einer regelmäßigen Legitimierung der Datenverarbeitungsmaßnahmen. Nicht zutreffend ist sicherlich die Annahme, die Widerspruchsmöglichkeit des Betroffenen gegen Datenverarbeitungen zum Zwecke der Werbung gem. § 28 Abs. 4 S. 1 BDSG weise darauf hin, dass die Verantwortliche Stelle grundsätzlich ein vorrangiges berechtigtes Interesse an Datenverarbeitungen habe.[602] Vielmehr lässt sich aus dem grundsätzlichen Erfordernis der Einwilligung des Betroffenen in solche Datenverarbeitungsmaßnahmen ableiten, dass im Zweifel dessen Interessen überwiegen.[603] Die Widerspruchsmöglichkeit soll seine Rechte daher auch zusätzlich sichern und nicht dazu führen, dass ihm diese *a priori* aberkannt und sie ihm nur zuerkannt werden, sofern er sich aktiv mittels Widerspruch wehrt. Die Zweifelsfallregelung muss sich vor dem Hintergrund der Bedeutung des durch das Grundgesetz gewährten Rechts auf informationelle Selbstbestimmung an den Interessen der Betroffenen orientieren und kann daher im Ergebnis nur dahingehen, dass die Datenverarbeitung *im Zweifel* zu unterbleiben hat, sofern unklar ist, ob schutzwürdige Interessen der Betroffenen nicht doch überwiegen.[604]

In RFID-Anwendungen ließe sich gegebenenfalls ein Kompromiss dahingehend finden, dass die Beteiligten zusammen‘arbeiten’. Ohne vorherige Information des Betroffenen über das Vorhandensein und die Nutzung der RFID-Infrastruktur zwecks Datenerhebung und -verarbeitung weiß dieser im Zweifel nicht einmal, dass seine schutzwürdigen Belange betroffen sein könnten. Da diese Belange bei jedem Betroffenen divergieren, drängen sich eben diese folglich auch der verantwortlichen Stelle nicht auf. Sofern vom Betroffenen unbemerkte Ortungen und Profilierungen seitens der verantwortlichen Stelle also gerade nicht im Vertrag geregelt sind, könnte über entsprechende Hinweisschilder an neuralgischen Punkten – etwa am Eingang zu öffentlichen Nahverkehrsmitteln – eine entsprechende Information durchgeführt werden. Hierauf hin kann sich jeder Betroffene überlegen, ob er die entsprechende Datenverarbeitung akzeptieren oder ob er seinen entgegenstehenden Willen und etwaige schutzwürdige Interessen der verantwortlichen Stelle mitteilen möchte. Ein solcher Ansatz wird wie angesprochen auch mit der Empfehlung der Kommission[605] verfolgt.[606]

Eine Rechtfertigung der über den Vertragszweck hinausgehenden Nutzung der Daten über § 28 Abs. 1 S. 1 Nr. 3 BDSG dürfte bei ÖPNV-Tickets und ähnlichem ausscheiden. Die Da-

---

[601] *Simitis* in: Simitis, BDSG, § 28 Rn. 165.

[602] So aber *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 140.

[603] So auch *Simitis* in: Simitis, BDSG, § 28 Rn. 164, 165.

[604] *Simitis* in: Simitis, BDSG, § 28 Rn. 166.

[605] Empfehlung 2009/387/EG, oben Fn. 2.

[606] Hierzu unten E.II.1.

ten sind schließlich gerade nicht öffentlich zugänglich, sondern werden erst von der verantwortlichen Stelle beim Betroffenen erhoben und dann gegebenenfalls auf dem Tag gespeichert. Eine pauschale Veröffentlichungsbefugnis ist mangels gesetzlicher Erlaubnis ebenfalls zu verneinen. Eine solche hinge vielmehr von der Einwilligung des Betroffenen ab.

Szenario 2

(2) RTAMP – Intrinsic Ubiquity:

Auf dem RFID-Tag ist nur eine einzigartige Identifikationsnummer gespeichert, das RFID-Tag ist aber mit dem menschlichen Körper verbunden (VeriChip o.ä.) und in einem Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert.

Bei der Bewertung der Rechtmäßigkeit von Datenverarbeitungsmaßnahmen i.R.v. Szenario 2 ist wiederum vorranging auf das vorliegende Vertragsverhältnis und den mit ihm verbundenen Zweck abzustellen. Implantierte oder anderweitig fest mit dem menschlichen Körper verbundene RFID-Tags (dies können beispielsweise auch nicht ablegbare Armbänder o.ä. sein) in der Privatwirtschaft bieten sich insbesondere im Gesundheitswesen an. Aber auch die „implantierte Geldbörse“ könnte ein ernstzunehmender Anwendungsfall werden.

Ärztlichen Behandlungen liegt ein Behandlungsvertrag zugrunde. Die Aushändigung von RFID-Tags wird mangels weitergehenden Bedarfs wohl nur bei stationären Behandlungen oder im Rahmen von Heimaufenthalten etwa bei alten oder behinderten Personen in Betracht kommen. Die Verarbeitung der auf diesen Tags gespeicherten Daten muss gleichfalls wieder zur Erreichung des mit dem Vertrag verfolgten Zwecks erforderlich sein. Primärer Zweck eines Behandlungsvertrags ist soweit wie möglich die Wiederherstellung der Gesundheit, bei Pflegeverträgen jedenfalls die Aufrechterhaltung des *status quo* und die Pflege des Betroffenen. Von diesen Vertragszwecken umfasst ist sicher das Auslesen der Tag-Daten zum Abgleich mit den im Hintergrundsystem gespeicherten Daten in medizinischen Notfällen. Auch die Auslesung im Rahmen der täglichen Visite ist jedenfalls dann vom Vertragszweck umfasst, sofern das System der Einrichtung darauf ausgelegt ist, mittels Auslesung der Identifikationsnummer Einblick in die Krankenakte des Patienten zu erhalten. Anders stellt sich die Beurteilung dar, sofern im gesamten Klinikbereich Kontroll-Lesegeräte installiert sind, mittels derer der Aufenthalt und die Bewegung der Patienten pauschal nachvollzogen und protokollieret wird, also Bewegungsprofile angelegt werden. Eine solche Überwachung ist nur dann über § 28 Abs. 1 S. 1 Nr. 1 BDSG zu rechtfertigen, wenn sie medizinisch indiziert, also zur Erreichung des Vertragsziels erforderlich ist. Dies gilt mitnichten bei allen Patienten, so z.B. nicht bei solchen, die nicht schwer krank, ansprechbar und zurechnungsfähig sind. Für den Behandlungserfolg bei Patienten mit stetigem Komplikationsrisiko oder solchen, die verwirrt oder unzurechnungsfähig sind, wird eine dauerhafte Kontrolle des Aufenthalts indes erforderlich sein.[607]

Neben dem Vertragszweck bestehende berechtigte Interessen medizinischer Einrichtungen i.S.v. § 28 Abs. 1 S. 1 Nr. 2 BDSG ihre Patienten dauerhaft zu orten und damit zu überwachen, sind schwer vorstellbar. Inwiefern wirtschaftliche Interessen der Klinik – etwa an einem

[607] *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 137.

effizienteren Ablauf – mit solch stetigen Überwachungsmaßnahmen bedient werden könnten, ist nicht ersichtlich.

Bei der „Geldbörse unter der Haut" sind zwei unterschiedliche Vertragsverhältnisse zu berücksichtigen. Einerseits besteht ein solches mit dem Unternehmen, welches den Bezahlservice und damit auch die Implantierung des Tags anbietet und andererseits der jeweilige Verkäufer oder Dienstleister, der über die mittels des RFID-Tags zugänglichen Bankdaten – im Hintergrundsystem – abrechnen möchte. Wichtig ist das Vertragsverhältnis mit dem jeweiligen Verkäufer oder Dienstleister. Dieser darf dem Vertrag nach zwecks Abrechnung das Tag auslesen oder auch – wie im Fall des Baja Beachclubs – zwecks Überprüfung der Legitimation zum Eintritt in den VIP-Bereich. Hierüber hinausgehende Ortungs-oder Profilierungsmaßnahmen sind nicht vom Vertrag umfasst. Auch hier sind berechtigte Interessen, die neben dem Vertrag bestehen, schwer vorstellbar, können aber im Einzelfall sicher bestehen.

Szenario 3

(3) EPC-AGG:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige Identifikationsnummer gespeichert; im Hintergrundsystem sind personenbezogene Daten wie Name, Anschrift etc. gespeichert (z.B. Kundenkarte, Türöffner etc.); der Gegenstand wird regelmäßig von Personen mitgeführt.

RFID-Tags i.S.v. Szenario 3 werden an die Betroffenen ebenfalls ausgegeben, um einen bestimmten vertraglichen Zweck zu erfüllen. Bei Kundenkarten ist dies die Gutschrift von Punkten oder die Gewährung von Rabatten. Die Gewährung dieser Leistungen an den Kunden erfordern die Erhebung der Kundenkartendaten, damit die Leistung auf dem Punktekonto des Kunden gutgeschrieben werden kann. Inwiefern die verantwortliche Stelle darüber hinaus berechtigt ist, das Kaufverhalten mittels Protokollierung der vom Betroffenen gekauften Produkte zu analysieren, ist überdies nicht zu klären im Rahmen der Auslesung der Kundenkartenidentifikationsnummer an der Kasse. Es geht hierbei vielmehr um die Frage, ob die Zusammenführung der Daten über das Kaufverhalten eines anonymen Kunden mit den Daten der Kundenkarte – welche die Analyse erst zu einer personalisierten macht – durch den Zweck des Kundenkartenvertrags gedeckt ist (AGG-Szenario). Die Rechtmäßigkeit dieser Zusammenführung richtet sich demnach zwar ebenfalls nach dem zugrundeliegenden Kundenkartenvertrag, sie ist aber losgelöst von der Auslesung des RFID-Tags als solchem zu betrachten.[608] Es ist auch darauf hinzuweisen, dass die aus einer entsprechenden Zusammenführung der Daten herrührenden Gefahren keine RFID-spezifischen sind. Sie treten genauso – bereits heute – im Zusammenhang mit Kundenkarten auf Barcode- oder Magnetstreifenbasis auf.

Problematischer stellen sich die Auslesevorgänge dar, die unabhängig vom Kassiervorgang, also auf der Verkaufsfläche durchgeführt werden könnten. Solche werden kaum von einem Kundenbindungsvertrag umfasst sein, geht es doch um eine umfangreiche Profilierung, ohne

[608] Vgl. weiterführend Unabhängiges Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Kundenbindungssysteme und Datenschutz, abrufbar unter https://www.datenschutzzentrum.de/wirtschaft/Kundenbindungssysteme.pdf (04.04.2013).

dass den Betroffenen hierfür eine Gegenleistung – die ja gerade Anreiz für den Abschluss des Kundenkartenvertrags war – geboten wird. Hinzukommend kann sich der Betroffene nicht mehr der Datenerhebung entziehen, weil er von der Positionierung der Lesegräte keine Kenntnis hat (an der Kasse erwartet er jedenfalls, dass seine Daten ausgelesen werden). Entsprechend scheitert eine Rechtfertigung über § 28 Abs. 1 S. 1 Nr. 1 BDSG bei stetiger Ortung und Profilierung mittels der Kundenkartenidentifikationsnummer.[609]

Hinsichtlich der Rechtfertigung wegen berechtigter Interessen der verantwortlichen Stelle gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG kann auf die Ausführungen im Rahmen von Szenario 1 beim ÖPNV-Ticket verwiesen werden. Die Tatsache, dass bei der Kundenkarte lediglich eine Identifikationsnummer gespeichert ist, macht wie gesehen keinen Unterschied, weil diese Nummer nach derzeit gültiger Definition und diesseitiger Auslegung derselben ebenfalls personenbezogenes Datum und sie mithin genauso zu behandeln ist, wie konventionelle Identifikatoren. Insbesondere das potenziell überwiegende schutzwürdige Interesse der Betroffenen an der Nichterfassung der Daten auf der Verkaufsfläche dürfte hier Zweifel an einer Rechtfertigungsmöglichkeit aufkommen lassen. Hinzukommend sind bei der Erstellung von Profilen zwecks Schaltung kundensensitiver Werbung § 28 Abs. 3 bis 4 BDSG zu berücksichtigen, die besondere Regelungen für die Datenverarbeitung zu Werbezwecken vorsehen. Nach § 28 Abs. 3 BDSG ist eine Datenerhebung zu Zwecken der Werbung grundsätzlich nur zulässig, sofern der Betroffene hierfür seine Einwilligung erteilt hat.

Szenario 4

(4) EPC:

Auf dem RFID-Tag, welches mit einem Gegenstand verbunden ist, ist nur eine einzigartige (produktbezogene) Identifikationsnummer gespeichert; im Hintergrundsystem sind nur weiterführende Daten zum Produkt gespeichert; der Gegenstand wird vorübergehend oder regelmäßig von Personen mitgeführt.

Eine Rechtfertigung von Datenverarbeitungsmaßnahmen i.R.v. Szenario 4 im Einzelhandel – maßgeblich zur Erstellung von Bewegungs- und Kundenprofilen zur Optimierung von Geschäftsprozessen und zur Schaltung kundensensitiver Werbung – gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG stößt zunächst auf die Herausforderung, dass zum Zeitpunkt der Datenerhebung auf der Ladenfläche noch gar kein Vertrag mit der verantwortlichen Stelle geschlossen worden ist.[610] Dieser (Kauf-)Vertrag kommt erst beim Bezahlen an der Kasse zu Stande. Ein vorvertragliches Schuldverhältnis i.S. einer Vertragsanbahnung gem. § 311 Abs. 2 Nr. 2 BGB besteht indes bereits vorher, nämlich mit Betreten des Geschäfts durch den Kunden.[611]

---

[609] Vgl. auch *v. Westerhold/Döring*, CR 2004, 710 (712 f.); *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 138.

[610] Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 206, lehnen daher auch die Anwendbarkeit von § 28 Abs. 1 S. 1 Nr. 1 BDSG ab.

[611] Vgl. auch *v. Westerhold/Döring*, CR 2004, 710 (712 f.); *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 138.

Eine Rechtfertigung über § 28 Abs. 1 S. 1 Nr. 1 BDSG ist zum Einen möglich, sofern die Datenverarbeitungsmaßnahme zur Begründung eines rechtsgeschäftlichen Schuldverhältnisses – namentlich der an der Kasse abzuschließende Kaufvertrag – aber auch zur Durchführung eines rechtsgeschäftsähnlichen Schuldverhältnisses – in diesem Fall die Vertragsanbahnung – erforderlich ist. Die erste Alternative scheint fernliegend, ist doch zum Abschluss des Kaufvertrags zwischen Betroffenem und verantwortlicher Stelle nicht erforderlich, dass im vorvertraglichen Stadium Bewegungsprofile des Betroffenen angefertigt werden. Dies gilt gleichermaßen für Daten, die zu Werbezwecken erhoben werden sollen. Auch im Rahmen der Durchführung des vorvertraglichen Stadiums, der Vertragsanbahnung, ist eine Profilierung nicht Gegenstand der Zweckbestimmung und entsprechend nicht erforderlich. Die Zweckbestimmung der Vertragsanbahnung ist der Abschluss des entsprechenden Kaufvertrags – nicht hingegen die Ortung der Kunden zwecks Geschäftsoptimierung oder zu Marketingzwecken.[612] Eine Rechtfertigung von Profilierungsmaßnahmen sowohl vor als auch nach Abschluss des Kaufvertrags mit der verantwortlichen Stelle über § 28 Abs. 1 S. 1 Nr. 1 BDSG scheidet damit aus. Die Erhebung der Produktdaten zu Zwecken der sensitiven Werbung müsste überdies die besonderen Voraussetzungen des § 28 Abs. 3-5 BDSG erfüllen. Dies erforderte insbesondere die Einholung der Einwilligung aller Betroffenen vor der Erhebung, was – wie bereits an vielen Stellen deutlich geworden – impraktikabel wäre und von den Kunden kaum angenommen werden dürfte.

Die verantwortliche Stelle hat allerdings aus wirtschaftlichen Gründen ein durchaus berechtigtes Interesse an der Erhebung und Weiterverarbeitung der betreffenden Produktdaten, jedenfalls soweit der Erhebungszweck von vornherein bestimmt ist. Insoweit käme eine Rechtfertigung gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG in Betracht. Auch in Szenario 4 dürften indes im Zweifel überwiegende schutzwürdigen Interessen der Betroffenen am Ausschluss der Verarbeitung gegen diese sprechen.[613] Hierbei kann auf oben zu Szenario 1 Gesagtes verwiesen werden. In RFID-Anwendungen i.S.v. Szenario 4 könnte ein Kompromiss wiederum durch eine Mittelweglösung erreicht werden: Hinweise wie auch von § 6c Abs. 1 BDSG gefordert – etwa am Eingang des Geschäfts und an den jeweiligen Lesegeräten – weisen die Kunden auf die vorhandene RFID-Infrastruktur und die geplante Datenerhebung hin und ermöglichen die Kundgabe entgegenstehender Kundeninteressen. Ohne ein solches Vorgehen ist mit oben gesagtem *im Zweifel* davon auszugehen, dass entgegenstehende schutzwürdige Interessen der Betroffenen überwiegen, was wiederum dazu führte, dass Datenerhebungen und -verarbeitungen i.S.v. Szenario 4 im Zweifel rechtswidrig wären. Bereits aus wirtschaftlichen Interessen der verantwortlichen Stellen ist von daher ein „Zugehen“ auf die Kunden zu empfehlen.

---

[612] So auch *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 138, der diese Einschätzung allerdings für das (noch gar nicht bestehende) Vertragsverhältnis abgibt; ebenso Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 215.

[613] So auch Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 206.

Eine Rechtfertigung der Datenverarbeitungsmaßnahmen gem. § 28 Abs. 1 S. 1 Nr. 3 BDSG ist auch in Szenario 4 abzulehnen. Nr. 3 fordert allgemein zugängliche Daten. Bei Fehlen entsprechender Verschlüsselungsmechanismen könnte man geneigt sein, die auf RFID-Tags grundsätzlich dieser Kategorie zuzuordnen, weil sie schließlich jedermann mit kompatiblem Lesegerät auslesen kann. Hierbei ist aber zu bedenken, dass allgemein zugängliche Daten i.S.d. Norm nur solche sind, die sowohl ihrer technischen Ausgestaltung nach – dies wäre bei fehlender Verschlüsselung zu bejahen – als auch ihrer *Zielsetzung* nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[614] Diese Zielsetzung lässt sich auch bei Produktidentifikationsnummern in massenhafter Verbreitung nicht erkennen: Die bloße Möglichkeit der Auslesung durch jedermann indiziert noch nicht, dass dies auch die Zielsetzung ist. Vielmehr ist diese Möglichkeit eine technikimmanente Eigenschaft. Ausgelesen werden sollen die Tags nach der Zielsetzung der jeweiligen Verwender – also Produzenten – nur von den Stellen, die an der Vermarktung der Produkte beteiligt sind. Unbeteiligte Dritte, die eine eigene RFID-Infrastruktur betreiben oder gar mit mobilen Lesegeräten die Betroffenen auf der Straße ausspähen, sind von dieser Zielsetzung nicht umfasst.

III. Zusammenfassung und Fazit

Auf die benannten RFID-Szenarien finden bereits heute – sowohl spezialgesetzliche als auch allgemeine – datenschutzrechtliche Regelungen Anwendung. Weniger problematisch stellen sich die Szenarien dar, in denen der Gesetzgeber detaillierte Regelungen zum Einsatz von RFID geschaffen hat, wie im PassG und PAuswG. Zwar wird es hier in der Zukunft darauf ankommen, dass die technischen Vorgaben stetig überprüft, angepasst und vor allem eingehalten werden, um ein höchstmögliches Maß an Datensicherheit und damit Datenschutz zu garantieren. Indes ergeben sich nicht bereits auf Ebene der Gesetzesanwendung Herausforderungen, wie sie sich im Bereich der Anwendung der allgemeinen Datenschutzgesetze herauskristallisieren.

In privatwirtschaftlichen RFID-Anwendungen ist auf das BDSG abzustellen, welches die grundgesetzlichen Vorgaben zum Schutz des informationellen Selbstbestimmungsrechts umsetzt. Es zeichnet sich immer mehr ab, dass dieser gesetzliche Rahmen den Herausforderungen der dargestellten Anwendungen nicht mehr hinreichend begegnen kann. Das Konzept des – jahrzehntealten – europäischen und deutschen Datenschutzes orientiert sich an einer Situation, in der die Erhebung personenbezogener Daten manuell beim Betroffenen stattfand und elektronische Verarbeitungsmaßnahmen in von wenigen Akteuren beherrschten Rechenzentren erfolgten. Die Verhältnisse waren damit überschaubar: Elektronische Datenverarbeitung betraf lediglich klar abgrenzbare Einzelfälle, in denen wenige Beteiligte Daten anhand klarer Prozesse zu festgelegten Zwecken verarbeiteten.[615] Die sich hieraus ergebende Transparenz bewirkte eine weitgehende Kontrollmöglichkeit des Betroffenen.[616] Der gesetzliche Rahmen

---

[614] *Simitis* in: Simitis, BDSG, § 28 Rn. 189.

[615] *Roßnagel*, Datenschutz in einem informatisierten Alltag, abrufbar unter http://library.fes.de/pdf-files/stabsabteilung/04548.pdf (04.04.2013), S. 120.

[616] *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 106.

stieß bereits mit Entstehung und fortwährender Weiterentwicklung des Internet an seine Grenzen: Die von den Betroffenen durch ihre IP-Adressen[617] hinterlassenen Datenspuren sind von ihnen nicht nachvollziehbar und die weitergehende Verwendung dieser Daten von ihnen nicht kontrollierbar. Wirksamen Schutz ihres Persönlichkeitsrechts im Zusammenhang mit dem Internet können die Betroffenen allerdings immer noch darüber erhalten, indem sie das Medium – was zugebenermaßen immer schwieriger wird – nicht nutzen.[618]

Eine solche Entzugsmöglichkeit wird es in einer Welt des *ubiquitous computing* nicht mehr geben. Sich einer allgegenwärtigen RFID-Infrastruktur zu entziehen ist zwar theoretisch denkbar praktisch aber kaum möglich. Außerdem würden durch eine Entziehung auch alle Vorteile von RFID beseitigt. Dies mögen Zweifler zwar unter Umständen gerne als notwendiges Übel in Kauf nehmen. Erstrebenswert ist aber, die Technik und ihre Anwendungen so zu gestalten, dass für die Betroffenen keine unerträglichen Beeinträchtigungen ihres Persönlichkeitsrechts drohen. Dies jedoch kann das bestehende allgemeine Datenschutzrecht nicht leisten:

Eine ubiquitäre Datenverarbeitungsstruktur zeichnet sich dadurch aus, dass eine unüberschaubare Anzahl an (verantwortlichen) Stellen eine enorme Anzahl an Einzeldatensätzen zu unterschiedlichsten Zwecken erhebt und verarbeitet und dies mittels RFID unbemerkt vom Betroffenen stattfindet.[619]

Die Herausforderungen, denen sich das bestehende Recht gegenübersieht, betreffen maßgeblich die Frage, ob und wenn ja wie weit die bestehenden Regelungen auf RFID-Systeme überhaupt Anwendung finden bzw. Bedingungen schaffen, mittels derer ein wirksamer Schutz des Persönlichkeitsrechts erreicht werden kann. Dies wurde zunächst besonders deutlich bei den Erörterungen zum Begriff der personenbezogenen Daten. Ob es sich bei einzelnen RFID-Daten um personenbezogene Daten i.S. datenschutzrechtlicher Regelungen handelt, wird in den meisten wissenschaftlichen Beiträgen pauschal und ohne weitere inhaltliche Auseinandersetzung mit dieser wesentlichen Frage beantwortet. Das Ergebnis fast aller herangezogenen Abhandlungen: Jedenfalls (produktbezogene) Identifikationsnummern auf RFID-Tags seien keine personenbezogenen Daten. Stimmte man dieser Ansicht zu, so wäre der künftig größte Anwendungsbereich für RFID nach heutiger Gesetzeslage datenschutzrechtlich irrelevant. Vor dem Hintergrund der in Teil C.II herausgearbeiteten Gefahren für das Persönlichkeitsrecht des Betroffenen auch bei solchen Anwendungen, müsste bei Annahme einer sol-

---

[617] Der EuGH hat in einem Vorlageverfahren zu der Frage, ob Internetzugangsprovider verpflichtet werden dürfen, Filtersysteme zur Unterbindung von Datenpiraterie einzusetzen, IP-Adressen als personenbezogene Daten qualifiziert, ohne hierbei zwischen dynamischen und statischen IP-Adressen zu unterscheiden oder sich mit den Voraussetzungen des Personenbezugs auseinanderzusetzen, EuGH Rs. C‑70/10, Urt. v. 24.11.2011, Rn. 51 = MMR 2012, 174; vgl. weiterhin zur Diskussion, ob IP-Adressen personenbezogene Daten sind *Meyerdierks*, MMR 2009, 8 ff.; für statsiche IP-Adressen: Taeger/Gabel/*Zscherpe*, § 15 TMG, Rn. 20; *Weichert* in: Däubler/Klebe/Wedde/Weichert, § 3 Rn. 14; für dynamische IP-Adressen: Taeger/Gabel/*Zscherpe*, § 15 TMG, Rn. 22.

[618] *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 107.

[619] *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 126.

chen Interpretation des Begriffs der personenbezogenen Daten wegen der auftretenden Regelungslücke selbiger folglich an die neuen Herausforderungen angepasst werden.[620]

Nach in dieser Arbeit vertretener und von der Artikel-29-Datenschutzgruppe geteilter Ansicht, ist dies indes nicht erforderlich. Vielmehr kann man im Wege der Auslegung dazu kommen, dass auch Identifikationsnummern auf produktbezogenen RFID-Tags als personenbezogene Daten zu qualifizieren und folglich in den Anwendungsbereich des Datenschutzrechts nach jetzigem Stand einbezogen sind. Dies hat aber auch zur Folge, dass bei der Verarbeitung produktbezogener Identifikationsnummern auf RFID-Tags sämtliche Vorgaben des BDSG zu beachten wären; dies stellte die Wirtschaft vor realistisch nicht zu bewältigende Aufgaben.

Bei der Anwendung des BDSG ergeben sich erhebliche Herausforderungen. Sehr deutlich wurde dies bei den Ausführungen zu § 6c BDSG, den die überwiegende Meinung jedenfalls bei produktbezogenen RFID-Tags, von denen Daten lediglich ausgelesen werden können, für nicht anwendbar hält.[621] Zwar kann nach hier vertretener Ansicht auch bei § 6c BDSG im Wege der Auslegung eine Anwendbarkeit auf alle RFID-Szenarien erreicht werden, indes erscheint es aus Gründen der Rechtssicherheit geboten, hier gesetzgeberisch nachzubessern und die bestehenden Unklarheiten auszuräumen.[622] In diesem Zusammenhang würde sich auch anbieten die bestehenden Transparenzpflichten zu konkretisieren, um sie an die Bedürfnisse in einer Welt ubiquitärer Datenverarbeitung anzupassen: Weil die individuelle Information jedes Betroffenen kaum handhabbar ist, könnte sie z.B. ersetzt werden durch die Möglichkeit zunächst breitenwirksame Hinweise bereitzustellen und die Aufforderung an die Betroffenen, sich weitergehend zu informieren, sofern dies gewünscht wird.[623]

Die Ausnahmeregelung zur Eröffnung des Anwendungsbereichs bei der Datenverarbeitung zu rein persönlichen oder familiären Tätigkeiten, § 1 Abs. 2 Nr. 3 BDSG, ist in einer ubiquitären Datenverarbeitungsstruktur nicht mehr vertretbar. Zwar ist richtig, dass bei rein persönlichen oder familiären Tätigkeiten das Gefahrpotenzial signifikant geringer ist als bei Datenverarbeitungen durch öffentliche Stellen oder im Rahmen ihrer Geschäftstätigkeit handelnder Wirtschaftsunternehmen. Allerdings kann auch eine auf RFID basierende „Nachbarüberwachung" zu erheblichen Beschränkungen des Persönlichkeitsrechts des Betroffenen führen.[624] Günstige

[620] So sehen dies die Vertreter der Fraktionen SPD, DIE LINKE und BÜNDNIS 90/DIE GRÜNEN in der Enquête-Kommission „Internet und Digitale Gesellschaft" im Zwischenbericht der Kommission zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 84; 98.

[621] Vgl. oben D.II.2.c)ee).

[622] *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 150, ist der Ansicht, dass wegen der Möglichkeit, unbemerkt vom Betroffenen einzugreifen, zumindest auch Tags mit zusätzlichem Speicher, die also nicht nur ausgelesen sondern auch beschrieben werden können, in den Anwendungsbereich von § 6c BDSG einzubeziehen sein sollen.

[623] S. schon oben D.II.2.c)hh)bbb) und D.II.2.e)dd); ähnlich *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 132; oder auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 85, die eine Abweichung von den bisherigen strengen Regeln zur individuellen Unterrichtung des Betroffenen – z.B. mittels Ersetzung derselben durch allgemeine Datenschutzerklärungen – nur bei bereits oben dargestellten Verarbeitungen ohne gezielten Personenbezug für erstrebenswert halten.

[624] *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 132.

und allgegenwärtig einsetzbare Infrastruktur könnte eine solche Überwachung möglich machen.

Datenverarbeitungen mittels Einwilligung des Betroffenen nach dem geltenden Verständnis zu legitimieren, wird in einer Welt des *ubiquitous computing* kaum mehr möglich sein. Nicht nur die formellen Anforderungen – insbesondere das Schriftformerfordernis – sind bei massenhafter Erhebung schlechterdings nicht einzuhalten, auch die Voraussetzung, dass der Betroffene seine Einwilligung freiwillig abgeben muss, wird bei allgegenwärtiger Datenverarbeitung mangels Entzugsmöglichkeit an ihre Grenzen stoßen[625], weil dem Betroffenen keine Wahlmöglichkeit mehr zwischen Abgabe der Einwilligung oder Verweigerung der selben verbleibt[626]. Weil die Einwilligung als Rechtfertigungstatbestand für die Datenverarbeitung die Einflussmöglichkeit des Betroffenen aber gerade gewährleisten soll, müssen entsprechende Anpassungen vorgenommen werden. In diesem Zusammenhang sollte darüber nachgedacht werden, der Einwilligung als direkten Ausfluss des informationellen Selbstbestimmungsrechts einen höheren Stellenwert einzuräumen und ihr eine deutliche vorrangige Stellung gegenüber den anderen Rechtfertigungsgründen zuweisen.[627]

Die Prinzipien der Zweckbindung, Erforderlichkeit und Datensparsamkeit stehen den technischen Entwicklungen im Bereich RFID und dem Ziel, allgegenwärtige Datenverarbeitung möglich zu machen, diametral gegenüber: Sofern Daten immer, überall und von jedermann erhoben werden können, sind diese Prinzipien nicht mehr einzuhalten. Bereits die Festlegung eines Erhebungszwecks, an dem sich dann auch alle späteren Verarbeitungsmaßnahmen zu orientieren haben, wird in vielen Fällen scheitern.[628]

Auch der Direkterhebungsgrundsatz dürfte bei einem flächendeckenden Einsatz von RFID nicht eingehalten werden können[629] – die Regelungen in § 4 Abs. 2 und 3 BDSG liefen damit leer. So stößt das Erfordernis der Kenntnis beim Betroffenen im Rahmen der bewussten Duldung auf die gleichen Herausforderungen wie die Transparenzpflichten, sodass auch hier entsprechender Anpassungsbedarf besteht. Den Bedürfnissen der ubiquitären Datenverarbeitung angepasst, könnten auch diese Transparenzpflichten so wie oben bei § 6c BDSG dargestellt ausgestaltet werden.

Die aufgezeigten Probleme im Bereich der Erlaubnistatbestände des § 28 Abs. 1 BDSG sind keine RFID-spezifischen, sie stellen sich bereits seit geraumer Zeit in verschiedensten Anwendungen. Insbesondere die Legitimierung mittels überwiegenden „berechtigten“ Interesses

---

[625] *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 137.

[626] So auch *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 151.

[627] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 72, 77.

[628] *Roßnagel*, Datenschutz in einem informatisierten Alltag, oben Fn. 615, S. 138 ff.; vgl. auch *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 153.

[629] Vgl. schon oben D.II.2.c)hh)bbb).

muss überdacht werden.[630] So sinnvoll es ist, die Vorschriften des BDSG so zu gestalten, dass möglichst alle denkbaren Szenarien darunter zu subsumieren sind, so wichtig ist es gerade aus diesem Grund, dass eine Subsumtion in der Praxis und nicht nur versierten Rechtsanwendern möglich ist. Für eine möglichst umfassende Einhaltung der datenschutzrechtlichen Regelungen ist es erforderlich, dass insbesondere den Betreibern von RFID-Systemen ihre Rechte und Pflichten deutlich sind. Je komplizierter das anzuwendende Recht ist, desto weniger Akzeptanz erfährt es schließlich bei seinen Adressaten.

Die aufgezeigten Schwachstellen machen einen wirksamen Schutz des Persönlichkeitsrechts der Betroffenen in einer Welt ubiquitärer RFID-Anwendungen unmöglich. Vor dem Hintergrund des objektiven Wertgehalts des Grundrechts und der hieraus erwachsenden Schutzpflicht des Staates, muss der Gesetzgeber tätig werden. Ob er die Schließung der bestehenden Schutzlücken mittels Anpassung der bestehenden Regeln gewährleistet, also im Wege einer Reformierung des allgemeinen Datenschutzrechts, oder durch Schaffung neuer bereichsspezifischer Gesetze, bleibt ihm überlassen. Bestrebungen des europäischen Gesetzgebers zur Überarbeitung der DSRL wurden bereits oben angesprochen.[631] Aber auch im Bereich der sektorspezifischen Regelungen gibt es Entwicklungen. Diese werden im nächsten Teil vorgestellt.

[630] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 77, die besonders bemängeln, dass bei Anlegung eines solchen Maßstabs, die dem Betroffenen zugesprochene Entscheidungsprärogative unterminiert wird.

[631] S. oben D.I.2.a)cc).

E. RFID-Datenschutzrecht – Neuer Ansatz

Neben der sowohl auf europäischer als auch deutscher Ebene angestrebten Reformierung des bestehenden technikneutralen Datenschutzrechts gibt es auch Vorstöße in Richtung RFID-spezifischer Regelungen. In der Diskussion ist die Schaffung solcher Regeln in Europa und Deutschland bereits seit mehreren Jahren (E.I). Der Europäische Gesetzgeber schaffte allerdings erst 2009 mit der Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen[632] eine Vorgabe, wie solche bereichsspezifischen Regelungen ansatzweise aussehen könnten (E.II). Auf deutscher Ebene hat es konkrete gesetzgeberische Ansätze bislang noch nicht gegeben. Indes werden auch hier immer wieder Forderungen nach einem RFID-Gesetz laut (E.III). Bemerkenswert sind vor dem Hintergrund der Zurückhaltung in der EU die seit Jahren anhaltenden Gesetzgebungsbestrebungen in den USA (E.IV).

I. Diskussionsstand

In den Fokus der Öffentlichkeit und vor allem verschiedener Interessenvertretungsgruppen aber auch der Datenschutzbeauftragten und des Gesetzgebers ist RFID bereits vor geraumer Zeit getreten. Der Anstoß zu einer kritischen Auseinandersetzung mit den datenschutzrechtlichen Herausforderungen von RFID kam aus den USA: Die US-amerikanische Verbraucherschutzorganisation CASPIAN (*Consumers Against Supermarket Privacy Invasion And Numbering*) rief bereits im März 2003 zum Boykott gegen die Verwendung von RFID-Tags auf Produktebene auf.[633]

Im November 2003 veröffentlichte das deutsche Pendent zu CASPIAN, der FoeBud e.V. (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs), ein Positionspapier zu RFID[634], indem er die Risiken aber auch politische Handlungsoptionen zur Begegnung dieser Risiken darstellt. Zusammenfassend fordert der FoeBud drei wesentliche Dinge: Vor der Einführung von RFID-Systemen muss eine umfassende Technikfolgenabschätzung durchgeführt werden, die RFID-Anwendung muss von einem Prinzip der fairen Informationspraxis geleitet sein und bestimmte RFID-Anwendungen sollten generell verboten werden.[635] Unter das Prinzip der fairen Informationspraxis fasst der FoeBud neben einer Auditierung („Sicherheitsbeurteilung"), strenger Einhaltung des Erforderlichkeits- und des Zweckbindungsgrundsatzes auch absolute Transparenz beim Einsatz von RFID-Systemen. Nach Auffassung des FoeBud muss die Information der Betroffenen so umfassend gestaltet sein, dass „jegliches Auslesen von Etiketten, das im Bereich des Handels erfolgt, allen Betei-

---

[632] Empfehlung 2009/387/EG, oben Fn. 2.

[633] Vgl. die Pressemitteilung von CASPIAN vom 12.03.2003, Consumer Group Calls for Immediate Worldwide Boycott of Benetton, abrufbar unter http://www.nocards.org/press/pressrelease03-12-03.shtml (04.04.2013).

[634] FoeBud, Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, vom 14.11.2003/19.11.2003, abrufbar unter http://www.foebud.org/rfid/unsere-positionen (04.04.2013).

[635] FoeBud, Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, vom 14.11.2003/19.11.2003, oben Fn. 634, S. 3.

ligten transparent“ ist, es also keinerlei heimliche Auslesevorgänge gibt.[636] Verbieten möchte der FoeBud sowohl jegliche Nutzungsverpflichtung – also ein Verbot oder Einschränkungen des Betroffenen als Folge der Deaktivierung oder Zerstörung der Tags – sowie das Anlegen von Profilen, es sei denn, der Betroffene stimmt ausdrücklich einer solchen Profilbildung zu.[637] Der FoeBud ist weiterhin sehr aktiv im Hinblick auf RFID. Zuletzt hat er im Januar 2012 mittels einer Aktion vor der GERRY WEBER Filiale in Bielefeld auf die Möglichkeit der Fernauslesung der in den Kleidungsstücken eingearbeiteten RFID-Tags aufmerksam gemacht.[638]

2004 haben die Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer 67. Konferenz eine Entschließung zu RFID verabschiedet.[639] In dieser nur zweiseitigen Entschließung weisen die Datenschutzbeauftragten bereits darauf hin, dass bei der Verwendung von RFID die Datenschutzprinzipien eingehalten werden müssen. Sie betonen unter anderem das Transparenzgebot, den Zweckbindungsgrundsatz sowie die Pflicht der Betreiber von RFID-Systemen, auf die Erhebung personenbezogener Daten zu verzichten, soweit sie nicht erforderlich sind. Auch eine Deaktivierungs- bzw. Zerstörungsmöglichkeit für die Betroffenen fordern die Datenschutzbeauftragten bereits damals. Sie weisen auch darauf hin, dass diese Grundsätze bereits beim Design von RFID-Systemen berücksichtigt werden müssen. Im Rahmen ihrer 72. Konferenz haben die Datenschutzbeauftragten eine zweite Entschließung zu RFID verabschiedet.[640] In dieser fordern die Datenschutzbeauftragten von den Herstellern und Betreibern von RFID-Systemen „alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten“; maßgeblich sei auf Transparenz, Kennzeichnungspflichten, das Verbot heimlicher Profilbildungen, den Schutz der gespeicherten Daten gegen unbefugte Kenntnisnahme sowie die Einräumung des Rechts des Betroffenen auf Deaktivierung oder Zerstörung der RFID-Tags hinzuwirken. Sie verweisen zunächst auf die Möglichkeit, dies in einer verbindlichen Selbstverpflichtung der Industrie umzusetzen. Für den Fall, dass die benannten Ziele nicht von der Wirtschaft selbst umgesetzt würden, müsse der Gesetzgeber den erforderlichen Rahmen gesetzlich festlegen. Der Bundesdatenschutzbeauftragte äußert sich ähnlich auch auf seiner Homepage und fordert Betreiber von RFID-Systemen im Einzelhandel hinzukommend zu den bereits genannten Zie-

---

636 FoeBud, Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, vom 14.11.2003/19.11.2003, oben Fn. 634, S. 4.

637 FoeBud, Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, vom 14.11.2003/19.11.2003, oben Fn. 634, S. 3 f.

638 Heise News Meldung, vom 16.01.2012, Funketiketten in der Kritik, abrufbar unter http://www.heise.de/newsticker/meldung/Funketiketten-in-der-Kritik-1414110.html (04.04.2013).

639 Entschließung 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken, Entschließung zu Radio-Frequency Identification vom 20.11.2003, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/67DSK-Radio-Frequency-Identification.pdf?__blob=publicationFile (04.04.2013).

640 Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg, „Verbindliche Regelungen für den Einsatz von RFID-Technologien“, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/72DSK-RFID.pdf?__blob=publicationFile (04.04.2013).

len dazu auf, wirksame Blockierungsmechanismen zu entwickeln, mit denen es möglich ist, das Auslesen der gespeicherten Daten zu unterbinden, sodass kein Nutzungszwang gegeben und das anonyme Einkaufen weiterhin möglich ist, sowie die Systeme und die zugehörigen Prozessabläufe einer Datenschutz-Auditierung zu unterziehen.[641] Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben sich in einem Beschluss aus dem Jahre 2006 ebenso wie die Datenschutzbeauftragten für eine datenschutzkonforme Gestaltung von RFID-Systemen insbesondere im Handel und Dienstleistungssektor ausgesprochen.[642] Auch sie fordern Transparenz, eine Kennzeichnungspflicht für RFID, die Möglichkeit zur Deaktivierung, die Sicherstellung der Vertraulichkeit des RFID-Systems sowie das Verbot heimlicher Profilbildungen.

Seitens der Wirtschaft hat sich insbesondere der BITKOM-Verband (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) als deren Vertreter hervorgetan. In einem Whitepaper zum Thema RFID aus dem Jahr 2005[643] weisen die Branchenvertreter mit Nachdruck darauf hin, dass eine erfolgreiche Einführung von RFID-Systemen maßgeblich von der Kundenakzeptanz abhängt; folglich müssten die Betreiber die geltenden Datenschutzbestimmungen zwingend einhalten.[644] Verantwortungsbewusstsein und Transparenz seien Grundvoraussetzungen beim Betrieb von RFID-Systemen, um dem Ziel der Unterstützung des informationellen Selbstbestimmungsrechts des Einzelnen gerecht zu werden. Zwar hält der BITKOM Bedrohungen bzw. Verletzungen der datenschutzrechtlichen Bestimmungenes durch die zum damaligen Zeitpunkt im Raum stehenden Anwendungen – dies dürfte indes auch für heutige Anwendungsszenarien gelten, hat sich in dem Bereich doch keine revolutionäre Entwicklung abgezeichnet – für nahezu ausgeschlossen, er weist aber dennoch auf das Erfordernis der Gewährleistung der Integrität und Vertraulichkeit der betroffenen Daten sowohl im Hinblick auf die Luftschnittstelle zwischen Tag und Reader aber auch zwischen Reader und Hintergrundsystem hin.[645] In einem Informationspapier zu RFID von 2004 nimmt der BITKOM dezidierter Stellung zu den datenschutzrechtlichen Herausforderungen der Technik.[646] Zunächst lehnt er es entgegen in dieser Arbeit vertretener Ansicht ab, produktbe-

---

641 Homepage des BfDI http://www.bfdi.bund.de/nn_530436/DE/Themen/TechnologischerDatenschutz/TechnologischeNeuerungen/Artikel/RFID-FunkchipsFuerJedeGelegenheit.html (04.04.2013).

642 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2006 in Bremen, Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich: Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/November06RFID.pdf?__blob=publicationFile (04.04.2013).

643 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74.

644 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 38.

645 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, oben Fn. 74, S. 39.

646 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, Informationspapier „Radio Frequency Identification (RFID) in der Diskussion – Technik, Einsatzformen, Datenschutz“

zogene Identifikationsnummern auf RFID-Tags als personenbezogene Daten zu qualifizieren. Es handele sich vielmehr um neutrale Daten, für die das geltende Datenschutzrecht keine Anwendung finde. Nichts desto trotz erkennt der BITKOM die öffentlichen Befürchtungen von Tracking und Profilbildung an und schlägt vor diesem Hintergrund vor, Hinweis- und Transparenzpflichten – umzusetzen beispielsweise durch Hinweisschilder, Aushänge und Piktogramme – für RFID-Anwendungen auf Produktebene einzuführen.[647] Auch die Einräumung eines Deaktivierungsanspruchs des Betroffenen gegenüber dem Betreiber – also der Tag ausgebenden Stelle – hält der BITKOM für sachgerecht.[648]

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat 2004 eine umfassende Studie zu den „Risiken und Chancen des Einsatzes von RFID-Systemen" veröffentlicht.[649] Die beteiligten Experten fordern Händler und Hersteller auf, „zunächst im Zuge eines freiwilligen Moratoriums auf den Einsatz von RFID bei Konsumgütern zu verzichten, bis in einer umfassenden Technikfolgenabschätzung alle Risiken und mögliche Gegenstrategien erarbeitet worden sind".[650] Die nach Ansicht der Experten bestehenden „erheblichen Gefährdungen" verdeutlichen sie mithilfe fiktiver Fallbeispiele, die das „Spannungsfeld zwischen Effizienz und Bequemlichkeit auf der einen und Sicherheit und Datenschutz auf der anderen Seite" aufzeigen.[651] Infolge der Möglichkeit des Tracking und der Anlegung umfassender Profile betonen die Experten die Wichtigkeit der Einhaltung der Grundsätze der Datensparsamkeit sowie schnellstmöglicher Anonymisierung bzw. Pseudonymisierung der Daten, der Zweckbindung sowie der Erforderlichkeit.[652]

Viele der von den verschiedenen Gruppen geforderten Maßnahmen sind bereits durch das bestehende Datenschutzrecht geregelt. So sind insbesondere die Grundsätze der Erforderlichkeit, der Datensparsamkeit und -vermeidung, der Zweckbindung aber auch das Datenschutzaudit im BDSG und der DSRL geregelt. Die von allen Beteiligten geforderte Transparenz beim Einsatz von RFID, umzusetzen durch umfassende Information des Betroffenen und Wahrung seines Auskunftsrechts, findet ebenfalls Anknüpfungspunkte in den bestehenden Datenschutzgesetzen. Auch Selbstverpflichtungen, die von der Wirtschaft abgeschlossen wer-

(2004), abrufbar unter http://www.bitkom.org/files/documents/BITKOM_RFID-Informationspapier_16.11.04.pdf (04.04.2013), S. 11 ff.

[647] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, Informationspapier „Radio Frequency Identification (RFID) in der Diskussion – Technik, Einsatzformen, Datenschutz" (2004), S. 13 f.

[648] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, Informationspapier „Radio Frequency Identification (RFID) in der Diskussion – Technik, Einsatzformen, Datenschutz" (2004), S. 14.

[649] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83.

[650] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 100.

[651] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 103 ff.

[652] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 24, 109 f.

den können, finden bereits einen Regelungsansatz im BDSG (§ 38a). Die in Teil D aufgezeigten Schwächen des bestehenden Rechts, haben indes auch die Gesetzgeber dazu bewegt, sich mit der Frage der Erforderlichkeit spezieller RFID-Datenschutzvorschriften zu befassen.

II. EU

Die Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen[653] (hiernach Empfehlung) ist der erste gesetzgeberische Akt in Bezug auf RFID auf EU-Ebene.

Im Folgenden sollen die wesentlichen Regelungsinhalte der Empfehlung dargestellt (E.II.1) sowie die Entwicklungsschritte zur Empfehlung skizziert werden (E.II.2). Hieran anschließend wird detailliert auf die in der Empfehlung geregelten Aspekte der Datenschutzfolgenabschätzung (E.II.3) sowie des Privacy-by-Design Ansatzes (E.II.4) eingegangen.

1. Empfehlung 2009/387/EG – Überblick

Die Empfehlung ist der bislang größte Schritt auf dem Weg einer RFID-Datenschutzgesetzgebung. Die Empfehlung hat allerdings – wie alle Empfehlungen – gemäß Artikel 288 AEUV (ex-Artikel 249 Abs. 5 EG) keine Bindungswirkung.[654] Sie dient vielmehr als programmatischer Leitfaden, der den Willen des europäischen Gesetzgebers zum Ausdruck bringen soll und den die Mitgliedstaaten jedenfalls berücksichtigen sollen.

In den Punkten 1. und 2. zum Anwendungsbereich stellt die Empfehlung klar:

> Anwendungsbereich
>
> 1. Diese Empfehlung gibt den Mitgliedstaaten Orientierungshilfen für die Gestaltung und den Betrieb von RFID-Anwendungen in einer rechtmäßigen und gesellschaftlich wie politisch annehmbaren Weise und unter Wahrung der Privatsphäre und Gewährleistung des Schutzes personenbezogener Daten.
>
> 2. Diese Empfehlung enthält Orientierungshilfen für Maßnahmen, die bei der Einführung von RFID-Anwendungen getroffen werden müssen, um sicherzustellen, dass die in Umsetzung der Richtlinien 95/46/EG, 1999/5/EG und 2002/58/EG erlassenen nationalen Rechtsvorschriften bei dieser Einführung, soweit zutreffend, eingehalten werden.

Diese Formulierung kann dahingehend interpretiert werden, dass die Kommission davon ausgeht, dass das bestehende Regelwerk – DSRL und eDSRL – ausreicht, um von RFID verursachten Datenschutzherausforderungen wirksam begegnen zu können. Vor diesem Hintergrund wäre die Empfehlung auch nicht als komplett neuer Gesetzgebungsansatz zu sehen, sondern als bloße RFID-spezifische *Interpretationshilfe* für das bereits bestehende Datenschutzrecht.

Die Empfehlung definiert unter Punkt drei wichtige Begriffe. Von besonderem Interesse ist die Definition für RFID, Punkt 3 (a) der Empfehlung:

> a) „Funkwellenidentifikation“ (RFID) ist die Nutzung elektromagnetischer Wellen oder der elektromagnetischen Nachfeldkopplung im Funkbereich des Frequenzspektrums für die Kommunikation von oder zu einem RFID-Tag mit Hilfe verschiedener Modulations- oder Kodierungstechniken oder nur für das Auslesen der Kennung eines RFID-Tags oder anderer darin gespeicherter Daten;

---

[653] Empfehlung 2009/387/EG, oben Fn. 2.

[654] Vgl. auch *Huber*, MMR 2008, VI (VIII).

In Punkt 3 g) wird der Begriff der Überwachung definiert:

> g) „Überwachung“ ist jede Tätigkeit zur Ermittlung, Beobachtung, Kopie oder Aufzeichnung des Aufenthaltsorts, der Bewegung, der Tätigkeiten oder des Zustands einer Person.

Der europäische Gesetzgeber erkennt damit eine der wesentlichen Herausforderungen der RFID-Technik – wie sie auch in dieser Arbeit herausgearbeitet wurde, s.o. C.II – an.

Die wesentlichen Ziele der Empfehlung sind:

- Erstellung eines Rahmens für Datenschutzfolgenabschätzungen (a),
- Information und Transparenz (b),
- Besondere Regeln für RFID-Anwendungen im Einzelhandel (c), und
- Stärkung des *Privacy-by-Design*-Ansatzes (d).

a) Datenschutzfolgenabschätzung für RFID-Anwendungen

Das erste wichtige Ziel der Empfehlung ist die Schaffung einer Grundlage für Selbstregulierungsmaßnahmen der Wirtschaft. Zu diesem Zwecke fordert Punkt 4 der Empfehlung von den Mitgliedstaaten:

> 4. Die Mitgliedstaaten sollten dafür sorgen, dass die Branche in Zusammenarbeit mit den jeweiligen Beteiligten aus der Zivilgesellschaft einen Rahmen für Datenschutzfolgenabschätzungen aufstellt. Dieser Rahmen sollte der Artikel- 29-Datenschutzgruppe innerhalb von 12 Monaten nach Veröffentlichung dieser Empfehlung im Amtsblatt der Europäischen Union zur Prüfung vorgelegt werden.

Im März 2010 legte die Branche der Artikel-29-Datenschutzgruppe einen ersten Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen vor.[655] Dieser erste Vorschlag wurde von der Datenschutzgruppe in einer entsprechenden Stellungnahme vom 13. Juli 2010 in der vorgelegten Form nicht befürwortet.[656] Daraufhin überarbeitete die Branche ihren Vorschlag und legte der Datenschutzgruppe diesen zweiten Entwurf[657] im Januar 2011 zur erneuten Prüfung vor. Dieser zweite Rahmen wurde von der Artikel-29-Datenschutzgruppe im Februar 2011 – wenn auch nicht vollkommen ohne inhaltliche Kritik – befürwortet[658] und am 6. April 2011 von der zuständigen Kommissarin *Neelie Kroes* unterzeichnet (mehr zum Rahmen für Datenschutzfolgenabschätzungen unten, E.II.3).

Aufbauend auf diesen Rahmen für eine Datenschutzfolgenabschätzung sollen die Mitgliedstaaten gem. Punkt 5 der Empfehlung dafür sorgen, dass Betreiber von RFID-Anwendungen für die betreffende Anwendung eine Datenschutzfolgenabschätzung anhand des entwickelten Rahmens durchführen, Punkt 5 a) und e), geeignete technische und organisatorische Maßnahmen zum Schutz des Persönlichkeitsrechts der Betroffenen treffen, Punkt 5 b), sowie einen Verantwortlichen oder eine Gruppe verantwortlicher Personen benennen, die für die

---

[655] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf (04.04.2013).

[656] Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323.

[657] Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 12.01.2011, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf (04.04.2013).

[658] Artikel-29-Datenschutzgruppe, WP 180, oben Fn. 339.

Durchführung der Datenschutzfolgenabschätzung und die dauerhafte Eignung der technischen und organisatorischen Maßnahmen verantwortlich ist, Punkt 5 c). Die Datenschutzfolgenabschätzung soll der zuständigen Behörde sechs Wochen vor Inbetriebnahme der Anwendung zur Verfügung gestellt werden, Punkt 5 d).

b) Information und Transparenz

Neben der Erstellung eines Rahmens für Datenschutzfolgenabschätzungen in RFID-Anwendungen führt die Empfehlung umfassende Transparenz- und Informationspflichten für die Betreiber von RFID-Anwendungen ein. Diese sollen gem. Punkt 7 der Empfehlung „für jede ihrer Anwendungen eine kurze, genaue und leicht verständliche Information ausarbeiten und veröffentlichen." Diese Information sollte mindestens enthalten:

- Name und Anschrift des Anbieters,
- Zweck der Anwendung,
- Art der Daten, die durch die Anwendung verarbeitet werden, anzugeben ist insbesondere, ob personenbezogene Daten verarbeitet werden und ob der Standort der RFID-Tags überwacht wird,
- Zusammenfassung der Datenschutzfolgenabschätzung,
- wahrscheinliche Risiken, die sich aus dem Einsatz von RFID-Tags in der Anwendung ergeben können, und Maßnahmen, die der Einzelne treffen kann, um diese Risiken zu mindern.

Hinzukommend sollen die Betreiber von RFID-Anwendungen dazu verpflichtet werden, auf die Präsenz von RFID-Lesegeräten hinzuweisen. Sie sollen hierfür ein europaweit einheitliches Zeichen verwenden, welches von der International Organisation for Standardization (ISO) entwickelt worden ist. [659] Das Zeichen soll den Namen des Betreibers und eine Anlaufstelle enthalten, bei der Einzelpersonen die oben genannte Information über die Anwendung erhalten können.

c) RFID im Einzelhandel

Für den Einsatz von RFID im Einzelhandel sieht die Empfehlung weitergehende Pflichten für die Betreiber der Systeme vor. Diese betreffen zum einen die Kennzeichnungspflicht, zum anderen die grundsätzliche Pflicht zur Deaktivierung oder Zerstörung der Tags noch am Verkaufsort.

aa) Einheitliches Zeichen

So soll sich der Empfehlung nach die Kennzeichnungspflicht, die in anderen Bereichen nur für Lesegeräte gilt, im Einzelhandel auch auf getaggte Produkte erstrecken, Punkt 9 der Emp-

[659] ISO/IEC FDIS 29160 Information technology -- Radio frequency identification for item management -- RFID Emblem, http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=040&ics3=&csnumber=45239 (04.04.2013).

fehlung. Entsprechend müsste auf alle mit einem RFID-Tag versehenen Produkte ein Warnhinweis aufgebracht werden, der auf die Präsenz des Tags hinweist.

bb) Deaktivierung und Zerstörung des Tags

Punkt 11 der Empfehlung stellt zudem die Forderung auf, dass der die RFID-Anwendung betreibende Einzelhändler grundsätzlich die verwendeten RFID-Tags am Verkaufsort deaktivieren oder entfernen soll, es sei denn, der Verbraucher stimmt nach Aufklärung der in Punkt 7 der Empfehlung genannten Punkte der weiteren Betriebsfähigkeit zu. Deaktivierung meint hierbei jedes Verfahren, das jede Wechselwirkung zwischen RFID-Tag und einem Lesegerät beendet und damit eine Datenauslesung unmöglich macht. Die Deaktivierung oder Entfernung der RFID-Tags soll sofort und für den Verbraucher kostenlos erfolgen. Zudem soll den Verbrauchern eine Überprüfungsmöglichkeit der erfolgreichen Deaktivierung bzw. Entfernung eingeräumt werden.

Für die Fälle, in denen die Datenschutzfolgenabschätzung ergibt, dass sich aus der weiteren Betriebsfähigkeit der RFID-Tags voraussichtlich keine Gefahren für das Persönlichkeitsrecht der Betroffenen ergeben wird, sind die Maßnahmen aus Punkt 11 der Empfehlung nicht zwingend anzuwenden, vgl. Punkt 12 der Empfehlung. Allerdings sollten die Betreiber der RFID-Anwendungen auch in diesen Fällen eine Möglichkeit zur sofortigen oder späteren Deaktivierung oder Entfernung der Tags kostenlos zur Verfügung stellen.

Punkt 13 der Empfehlung stellt klar, dass durch die Deaktivierung oder Entfernung der RFID-Tags die Rechtspflichten des Einzelhändlers gegenüber dem Verbraucher weder verringert noch aufgehoben werden dürfen, der Verbraucher also keine rechtlichen Nachteile durch die Deaktivierung oder Entfernung der Tags zu befürchten haben darf.

d) Privacy-by-Design

Die Empfehlung stellt weiterhin in Punkt 17 klar, dass im Zuge weitergehender Entwicklungsmaßnahmen im Bereich von RFID-Anwendungen schon frühzeitig der Grundsatz der eingebauten Sicherheit und Privatsphäre (*Privacy-by-Design*-Ansatz) berücksichtigt werden soll. Die Kommission hat bereits 2007 eine Mitteilung zur Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre veröffentlicht, in der sie unterschiedliche Techniken bespricht und sich der Förderung solcher Techniken verschreibt (mehr zu diesem Punkt unten, E.II.4).[660]

2. Der Weg zur Empfehlung

In den Erwägungsgründen zur Empfehlung bezieht sich die Kommission auf andere offizielle Dokumente verschiedener europäischer Stellen, die die Entwicklung der Empfehlung beeinflusst und teilweise Eingang in sie gefunden haben. Diese Materialien können daher als wertvolle Werkzeuge im Rahmen der Auslegung der Vorschriften der Empfehlung dienen; aus

[660] Mitteilung der Kommission an das Europäische Parlament und den Rat „über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre“, vom 02.05.2007, KOM(2007) 228 endgültig, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:DE:PDF (04.04.2013).

diesem Grund sollen sie im Folgenden kurz in chronologischer Entstehungsabfolge dargestellt werden. Die Kommission bezieht sich auf das Arbeitspapier der Artikel-29-Datenschutzgruppe zu Datenschutzfragen im Zusammenhang mit der RFID-Technik[661] (hiernach Arbeitspapier RFID), die Mitteilung der Kommission zu Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen[662] (hiernach Mitteilung zu RFID) und die Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung zu RFID[663] (hiernach EDSB Stellungnahme). Die folgende Darstellung beschränkt sich hierbei auf die für die Datenschutzdebatte relevanten Inhalte der jeweiligen Dokumente. Andere diskutierte Aspekte wie technische Harmonisierung, Umwelt- und Gesundheitsbedenken etc. sollen indes nicht besprochen werden.

Die Kommission berücksichtigt in den Erwägungsgründen zur Empfehlung weiterhin die Mitteilung der Kommission „Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung“[664] sowie die Entschließung des Rates zu einer Strategie für eine sichere Informationsgesellschaft in Europa[665]. Weil sich diese Dokumente nicht unmittelbar mit RFID beschäftigen, wird in dieser Arbeit nicht weiter auf sie eingegangen.

a) Arbeitspapier der Artikel-29-Datenschutzgruppe zu RFID

Im Januar 2005 veröffentlichte die Artikel-29-Datenschutzgruppe ein Arbeitspapier, welches sich mit den durch RFID bereits verursachten oder in der Zukunft entwickelnden Datenschutzherausforderungen beschäftigt. Das Arbeitspapier versteht sich hierbei als „Leitlinien für die Anwendung der in den EG-Richtlinien, insbesondere der Datenschutzrichtlinie, verankerten Grundprinzipien“.[666] Hieraus lässt sich der Rückschluss ziehen, dass die Datenschutzgruppe jedenfalls im Jahr 2005 noch keine Notwendigkeit für die Schaffung eines spezifischen RFID-Datenschutzgesetzes sah. Folglich bezieht sich das Dokument aber auch nur auf solche RFID-Anwendungen, in denen personenbezogene Daten verarbeitet werden – denn:

---

[661] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309.

[662] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zu „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“, KOM(2007) 96 endgültig, vom 15.03.2007, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:DE:PDF (04.04.2013).

[663] Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ (KOM(2007) 96), 2008/C 101/01, ABl. C 101/1 vom 23.04.2008, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_DE.pdf (04.04.2013).

[664] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung“, KOM(2006) 251 endgültig, vom 31.05.2006, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:DE:PDF (04.04.2013).

[665] Entschließung des Rates vom 22. März 2007 zu einer Strategie für eine sichere Informationsgesellschaft in Europa, 2007/C 68/01, Abl. C 68/1 vom 24.03.2007, abrufbar unter http://eur-lex.europa.eu/LexUriServ/site/de/oj/2007/c_068/c_06820070324de00010004.pdf (04.04.2013).

[666] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 8.

Nur in diesen Anwendungen greift der bestehende europäische Rechtsrahmen überhaupt erst ein. Dieser Punkt ist vor dem Hintergrund problematisch, dass – wie oben gezeigt – keine Einigkeit darüber besteht, ob produktbezogene Identifikationsnummern auf RFID-Tags als personenbezogene Daten zu qualifizieren sind oder nicht.

Bei den zu ergreifenden Maßnahmen zur Begegnung RFID-spezifischer Datenschutzherausforderungen weist die Datenschutzgruppe zunächst auf die allgemeinen Prinzipien der DSRL hin und betont, dass diese Prinzipien immer anwendbar sind, sofern die DSRL als solche anwendbar ist.[667] Die Datenschutzgruppe geht davon aus, dass nach geltendem Datenschutzrecht die Datenverarbeitungen in den meisten RFID-Anwendungen nur über die vorab einzuholende Einwilligung des Betroffenen zu rechtfertigen sein wird.[668]

Die bereits bestehenden Kennzeichnungspflichten der DSRL substantiiert die Datenschutzgruppe für das *product level tagging* im Einzelhandel dahingehend, dass Verbraucher über

- das Vorhandensein der RFID-Anwendung – sowohl die getaggten Produkte als auch die Situation der Lesegeräte –,
- die Folgen im Hinblick auf die Datenerhebung,
- die Zwecke, für die die Daten bestimmt sind,
- die Identität des für die Verarbeitung Verantwortlichen,
- Löschungs-, Deaktivierung- oder Entfernungsmöglichkeiten für die Tags sowie
- die Möglichkeiten der Wahrnehmung des Auskunftsrechts

informiert werden müssen.[669]

Die Datenschutzgruppe sieht hierbei die Notwendigkeit der Entwicklung eines einheitlichen Kennzeichens („Piktogramm“).[670] Die Informationspflichten sowie die Pflicht zur Verwendung eines standardisierten Kennzeichens haben Eingang in die Empfehlung gefunden.

Die Datenschutzgruppe widmet sich weiterhin eingehend den „technischen und organisatorischen Erfordernissen, die eine angemessene Verwirklichung der Datenschutzgrundsätze gewährleisten“. Bereits 2005 stellte sie fest, dass

> „beispielsweise mit der Normung des Aufbaus von RFID-Tag, -Lesegeräten und -Anwendungen erreicht werden [könnte], dass personenbezogene Daten sparsam erhoben und verwendet werden, und dass jedwede unrechtmäßige Verarbeitung verhindert wird, indem ein unautorisierter Zugriff auf personenbezogene Daten technisch vereitelt wird“ [671]

und formulierte damit den Mehrwert des *Privacy-by-Design*-Ansatzes in RFID-Anwendungen. Nach Ansicht der Datenschutzgruppe kann Technik hierbei in verschiedener

[667] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 10.

[668] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 11.

[669] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 12.

[670] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 15.

[671] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 13.

Hinsicht dem Datenschutz förderlich sein. Zum einen kann technische Normung neben der Interoperabilität auch dem Datenschutz zu Gute kommen.[672] Weiterhin soll auch bei der Wahrnehmung der Betroffenenrechte datenschutzfreundliche Technik zum Einsatz kommen können[673]; so könnte nach Ansicht der Datenschutzgruppe beispielsweise eine Löschfunktion in RFID-Tags eingebaut werden[674] und so die automatische Löschung der gespeicherten Daten bei Entfall der Rechtmäßigkeitsvoraussetzungen erreicht werden. Die Datenschutzgruppe nennt Beispiele, wie diese Deaktivierung durchgeführt werden kann.[675]

Sowohl die Weiterentwicklung des *Privacy-by-Design*-Ansatzes als auch die Ergreifung technischer und organisatorischer Maßnahmen zum Schutz von RFID-Infrastrukturen sieht die Kommission in ihrer Empfehlung vor. Während sie den *Privacy-by-Design*-Ansatz als neuen Grundsatz in die Empfehlung aufnimmt (Punkt 17 sowie Erwägungsgrund 6 der Empfehlung), betont sie, dass die Pflicht zur Ergreifung geeigneter technischer und organisatorischer Maßnahmen bereits nach der DSRL besteht und nimmt sie zur verstärkten Berücksichtigung in die zu erarbeitende Datenschutzfolgenabschätzung für RFID-Anwendungen auf (Punkt 5 b) und c) der Empfehlung).

Der Aspekt des Erfordernisses der Deaktivierung von RFID-Tags auf Produkten an der Kasse wurde von der Kommission in Punkt 11 der Empfehlung umgesetzt.

b) Mitteilung der Kommission zu RFID

2006 führte die Kommission eine öffentliche Online-Konsultation zu RFID durch. Die Ergebnisse dieser Konsultation sind wesentlicher Bestandteil der Mitteilung[676].

Eines der Ergebnisse der Konsultation ist die Erkenntnis, dass diverse Datenschutzbedenken im Zusammenhang mit RFID bestehen. Bemerkenswert ist, dass 55% der Teilnehmer der Konsultation der Ansicht waren, dass spezifische RFID-Datenschutzregelungen der beste Weg seien, den bestehenden und zu erwartenden Herausforderungen effektiv zu begegnen.[677] Die Kommission weist in diesem Zusammenhang bereits 2007 darauf hin, dass der bestehende Rechtsrahmen anwendbar ist, wenn in RFID-Anwendungen personenbezogene Daten verarbeitet werden; allerdings sieht sie auch die Notwendigkeit für Leitlinien, die verdeutlichen, wie das bestehende Recht konkret in RFID-Anwendungen anzuwenden ist.[678]

---

[672] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 13 ff.

[673] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 16 ff.

[674] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 17.

[675] Artikel-29-Datenschutzgruppe, WP 105, oben Fn. 309, S. 17 f.

[676] Mitteilung der Kommission, KOM(2007) 96 endgültig, oben Fn. 662.

[677] Mitteilung der Kommission, KOM(2007) 96 endgültig, oben Fn. 662, S. 5.

[678] Mitteilung der Kommission, KOM(2007) 96 endgültig, oben Fn. 662, S. 6 f.

Hinsichtlich der Sicherung von RFID-Anwendungen vertritt die Kommission bereits in der Mitteilung den Standpunkt zur Stärkung des *Privacy-by-Design*-Ansatzes, der später auch Eingang in Empfehlungsgrund 6 der Empfehlung gefunden hat.[679]

Zwecks weiterer Erörterung der Herausforderungen im Zusammenhang mit RFID und die weitergehende Koordinierung der Schritte zur Empfehlung setzte die Kommission per Beschluss eine „RFID-Sachverständigengruppe" ein[680], die die Kommission bezüglich des Inhalts der Empfehlung beriet (vgl. Art. 2 a) des Beschlusses).

c) Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission

Als Reaktion auf die Mitteilung der Kommission veröffentlichte der Europäische Datenschutzbeauftragte (EDSB) eine Stellungnahme zur Mitteilung.[681]

Die von der Kommission benannten Leitlinien zur Anwendungen des bestehenden Datenschutzrechts auf RFID-Anwendungen sollten nach Ansicht des EDSB einen sektorspezifischen Ansatz verfolgen:

> „Eine undifferenzierte Einheitslösung wird dem Anliegen, einen präzisen und kohärenten Rahmen zu gewährleisten, nicht dienlich sein."[682]

In der Empfehlung hat die Kommission indes lediglich für den Einzelhandel sektorspezifische Leitlinien entwickelt und diese sind nicht besonders umfangreich. Alle sonstigen RFID-Anwendungen haben sich bis jetzt lediglich an den allgemeinen Hinweisen der Empfehlung zu orientieren.

Ebenso wie die Artikel-29-Datenschutzgruppe weist auch der EDSB auf das Erfordernis der Einhaltung bereits bestehender datenschutzrechtlicher Anforderungen bei der Implementierung von RFID-Anwendungen hin. Maßgeblich müssten die Transparenz- und Informationspflichten sowie die Anforderungen an die Einwilligung des Betroffenen seitens der Betreiber der Anwendungen erfüllt werden.[683] In Anknüpfung an das Einwilligungserfordernis ist der EDSB der Ansicht, dass die geforderte Deaktivierung von RFID-Tags im Einzelhandel bereits unter den Grundsatz der Erlaubnisbedürftigkeit fällt: Das Unterlassen der Deaktivierung vor Verlassen der Verkaufsräume sei lediglich gerechtfertigt, wenn der Betroffene seine Einwilli-

---

[679] Mitteilung der Kommission, KOM(2007) 96 endgültig, oben Fn. 662, S. 10.

[680] Beschluss der Kommission vom 28.06.2007 zur Einsetzung der Sachverständigengruppe für Funkfrequenzkennzeichnung (RFID), 2007/467/EG, ABl. L 176/25 vom 06.07.2007, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:0030:de:PDF (04.04.2013).

[681] Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen" (KOM(2007) 96), 2008/C 101/01, ABl. C 101/1 vom 23.04.2008, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_DE.pdf (04.04.2013).

[682] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 41, S. 6.

[683] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 43, S. 6.

gung erteilt habe oder das Tag zur Erfüllung einer Dienstleistung seitens des Betreibers aktiv bleiben müsse (*Opt-In*-Prinzip).[684]

Ein weiterer vom EDSB angesprochener Themenkreis ist der des eingebauten Datenschutzes, also *Privacy-by-Design*. Hierauf bezieht sich die Kommission in ihrer Empfehlung ausdrücklich in Erwägungsgrund 12. Der EDSB fordert u.a. die Festlegung verbindlicher Normen zur Schaffung einheitlicher Ansätze bei der Verwirklichung des Grundsatzes des „eingebauten Datenschutzes" und fordert die Kommission auf hierbei eine aktive Rolle zu übernehmen.[685]

Kernpunkt der Stellungnahme des EDSB ist die Untersuchung der Frage, ob spezielle Rechtssetzungsmaßnahmen und gegebenenfalls sogar die Schaffung bereichsspezifischen RFID-Datenschutzrechts erforderlich ist.[686]

Bei der Untersuchung des bestehenden Rechtsrahmens zur Durchsetzung des Grundsatzes des „eingebauten Datenschutzes" weist der EDSB auf eine Regelung in der Richtlinie 1995/5/EG hin, die den Gebrauch von Funkanlagen und Telekommunikationsendeinrichtungen regelt. Nach Ansicht des EDSB sind die Mitgliedstaaten auch ohne Gesetzesänderung oder Neuschaffung bereichsspezifischer RFID-Regeln bereits jetzt auf Grundlage von Artikel 3 Abs. 3 c) Richtlinie 1995/5/EG in der Lage, den *Privacy-by-Design* Ansatz durchzusetzen.[687] Nach dieser Regelung kann die Kommission nach einem ebenfalls in der Richtlinie geregelten Verfahren festlegen, dass

> Artikel 3 Abs. 3 c) Richtlinie 1995/5/EG
>
> (…) Geräte in bestimmten Geräteklassen oder bestimmte Gerätetypen so hergestellt sein müssen, (…) dass sie über Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre des Benutzers und des Teilnehmers verfügen (…).

Ansonsten verbliebe die Anpassung der DSRL sowie der eDSRL in dieser Hinsicht.[688] Die eDSRL hat der europäische Gesetzgeber wie ausgeführt bereits dahingehend geändert, dass er verdeutlicht hat, dass selbige auch bei RFID-Anwendungen gilt, sofern diese an öffentliche Telekommunikationsnetze angeschlossen sind. Eine Anpassung der Richtlinien im Hinblick auf den *Privacy-by-Design* Ansatz hat es hingegen noch nicht gegeben.

Die Kommission hat stattdessen den Kompromiss gewählt, den *Privacy-by-Design*-Ansatz zunächst unverbindlich in die Empfehlung aufzunehmen. Der EDSB setzt sich in diesem Zusammenhang durchaus kritisch mit der Frage der Erforderlichkeit und Verhältnismäßigkeit neuer – verbindlicher – gesetzlicher Regelungen auseinander[689], aber auch mit Aspekten der Technologieneutralität und Rechtssicherheit[690]. Vor diesem Hintergrund betont der EDSB

---

[684] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 43, 46 ff., S. 6 f.

[685] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 54, S. 7.

[686] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 56 ff., S. 8.

[687] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 61, S. 8.

[688] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 62, S. 8.

[689] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 66, S. 9.

[690] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 67, S. 9.

auch, dass nicht jede technologische Entwicklung zu einer Anpassung der Datenschutzgesetze führen kann. [691] Allerdings rechnet er der RFID-Technologie durchaus eine Sonderrolle zu, die auch eine besondere Behandlung rechtfertige; der drohenden Entwicklung zur „Überwachungsgesellschaft", in der RFID eine tragende Rolle spielen könne, müsse wirksam begegnet werden können.[692] Entsprechend fordert der EDSB die Schaffung spezialgesetzlicher Regelungen sofern es nicht gelingt, den bestehenden Rechtsrahmen wirksam umzusetzen.[693] Weil dies in jedem Fall nicht bezüglich aller RFID-Anwendungen möglich sein wird – der EDSB bezieht sich hier auf alle Anwendungen, in denen keine personenbezogenen Daten verwendet werden und in denen das bestehende Datenschutzrecht mithin von vornherein keine Anwendung findet – aber auch diesen Anwendungen ein Überwachungspotenzial immanent sei, müssten gesetzliche Regelungen zumindest hier geschaffen werden.[694] Diese Forderung ist deshalb bemerkenswert, weil mit entsprechenden Regelungen, der Anwendungsbereich des bestehenden Datenschutzrechts maßgeblich erweitert bzw. ein „Quasi-Datenschutzrecht" geschaffen würde, das den Gefahren für das Persönlichkeitsrecht durch die Verarbeitung solcher „nicht-personenbezogenen" Daten begegnen sollte. Der Aspekt der Regelung auch solcher Anwendungen, in denen gerade keine personenbezogenen Daten verarbeitet werden, wird in der Empfehlung nicht aufgenommen.

Neue gesetzliche Regelungen sollten nach Ansicht des EDSB insbesondere den *Opt-In*-Ansatz sowie den *Privacy-by-Design*-Ansatz beinhalten.[695]

3. Selbstregulierung durch Datenschutzfolgenabschätzung

Obwohl keine dieser Stellungnahmen – nicht einmal die Mitteilung der Kommission – auf die Möglichkeit der Selbstregulierung eingeht, hat die Kommission in der Empfehlung die Branche zur Schaffung eines Rahmens für Datenschutzfolgenabschätzungen in RFID-Anwendungen aufgefordert, anhand dessen einzelne Unternehmen für ihre jeweilige RFID-Anwendung eine Datenschutzfolgenabschätzung durchführen sollen. Dieser Ansatz ist eine mögliche Form der Selbstregulierung. Selbstregulierung umfasst hierbei verschiedene Konzepte. Hierüber wird zunächst ein kurzer Überblick gegeben. Daran anschließend soll der Inhalt sowohl des ursprünglichen als auch des schlussendlich von der Artikel-29-Datenschutzgruppe befürworteten Vorschlags der Branche für einen Rahmen für Datenschutzfolgenabschätzungen sowie die von der Artikel-29-Datenschutzgruppe geäußerte Kritik dargestellt werden.

a) Selbstregulierung als Alternative zu Gesetzen

Selbstregulierung steht der Möglichkeit, gesetzliche Verhaltensvorgaben zu schaffen, gegenüber: Die Schaffung des Ausgleichs der Interessen von Betroffenem und verantwortlicher

[691] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 68, S. 9.

[692] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 69, S. 9.

[693] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 70, S. 10.

[694] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 74 f., S. 10.

[695] Stellungnahme des Europäischen Datenschutzbeauftragten, 2008/C 101/01, oben Fn. 681, Punkt 76, S. 10.

Stelle soll bei der reinen Selbstregulierung – im Gegensatz zur regulierten Selbstregulierung – ohne gesetzliche Regelung erreicht werden. Umgesetzt werden kann dieses Ziel zum einen durch vertragliche Regelungen zwischen der verantwortlichen Stelle und dem Einzelnen und/oder durch einseitig durch die verantwortliche Stelle oder einen Verband aufgestellte Verhaltensregeln, denen sich die verantwortliche Stelle unterwirft.[696] Als Überprüfungsinstanz kommt insbesondere die Durchführung von Auditverfahren mit anschließender Zertifizierung durch eine unabhängige Stelle in Betracht. Vorteile bringen Maßnahmen der Selbstregulierung im Bereich der Flexibilität.[697] Zum einen kann mithilfe individueller Regelungen schnell und unbürokratisch auf neue technische aber auch gesellschaftliche Entwicklungen reagiert werden, zum anderen kann auf die Besonderheiten des jeweiligen Unternehmens bzw. der Branche und der von diesen verwendeten Systeme eingegangen werden.[698] Hierdurch kann ein höheres Schutzniveau als durch starre gesetzliche Regeln erreicht werden. Dies gilt aber nur so lange, wie die verantwortliche Stelle nicht die Offenheit der gesetzlichen Regelungen einseitig zum eigenen Vorteil ausnutzt und dadurch die Rechte des Betroffenen einschränkt. Selbstregulierungsmaßnahmen sind von daher nur zulässig, wenn sie ein mindestens ebenso hohes Schutzniveau für das informationelle Selbstbestimmungsrecht des Einzelnen wie die staatliche Regulierung aufweisen.[699] Vor diesem Hintergrund sind gesetzesersetzende Selbstregulierungsmaßnahmen, die eine Beeinträchtigung des informationellen Selbstbestimmungsrechts zu rechtfertigen versuchen, unzulässig. Der Staat muss sich hier seinem Schutzauftrag entsprechend vor das informationelle Selbstbestimmungsrecht des Betroffenen stellen[700] und per Gesetz den Rahmen für zulässiges Verhalten in Bezug auf die Daten des Betroffenen abstecken.[701]

aa) Verhaltensregeln

Selbstregulierungsmaßnahmen durch Verhaltensregeln – sog. *Codes of Conduct* – werden sowohl vom europäischen als auch vom deutschen Datenschutzrecht vorgesehen. Gem. Artikel 27 Abs. 1 DSRL fördern die Kommission und die Mitgliedstaaten die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung der DSRL erlassen. Gemeint sind, wie sich aus Art. 27 Abs. 2 DSRL ergibt, Verhaltensregeln, die Berufsverbände und entsprechende Vereinigungen erarbeiten. Entsprechend regelt § 38a BDSG, dass Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Auf-

[696] *Polenz*, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, oben Fn. 78, S. 155.

[697] Vgl. Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 75.

[698] Vgl. auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 153.

[699] *Roßnagel* in: Roßnagel, HdB DSR, 3.6 Konzepte der Selbstregulierung, Rn. 18.

[700] Hierzu oben D.II.1.d).

[701] Vgl. hierzu *Roßnagel* in: Roßnagel, HdB DSR, 3.6 Konzepte der Selbstregulierung, Rn. 108; vgl. auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 154.

sichtsbehörde unterbreiten können. Wegen der Indisponibilität der europäischen und deutschen Datenschutzregelungen müssen sich solche Verhaltensregeln aber immer an das von der DSRL bzw. dem BDSG gewährleistete Mindestschutzniveau halten: Überschreitungen des Schutzniveaus sind möglich, Unterschreitungen zu Lasten des Betroffenen hingegen nicht.[702] Dies gebietet das verfassungsrechtlich gewährte Grundrecht auf informationelle Selbstbestimmung, für dessen Schutz der Gesetzgeber im Rahmen seines Gewährleistungsauftrags zu sorgen hat.[703] Verhaltensregeln können von daher nur zur konkreten branchenspezifischen Formulierung von Maßnahmen zur Einhaltung der gesetzlichen Standards – sozusagen als Interpretationshilfen[704] – verwendet werden, sie können die gesetzlichen Regeln indes nicht ersetzen.[705]

Nach der aktuellen Formulierung der DSRL und des BDSG ist die Selbstregulierung durch Verhaltensregeln der Wirtschaft nur eine Option und keine Pflicht. Die Pflicht zur Vorlage zwecks Überprüfung der erarbeiteten Verhaltensregeln betrifft überdies nur die Verhaltensregeln von Berufsverbänden und entsprechenden Vereinigungen. Verhaltenskodizes einzelner Unternehmen unterfallen diesem Kontrollinstrument nicht. Darüber hinaus müssen die erarbeiteten Verhaltensregeln nicht veröffentlich werden. Indem der Gesetzgeber dies nicht verbindlich fordert, vergibt er die Chance der Schaffung von Transparenz.[706]

In Betracht käme weiterhin die gesetzliche Verpflichtung zur Erarbeitung und Anwendung von Selbstverpflichtungen durch die Wirtschaft. Hierbei ist allerdings zu berücksichtigen, dass bei staatlich induzierter Selbstregulierung je nach Belastungseffekt auch grundrechtliche Abwehrrechte durch die verpflichteten Unternehmen geltend gemacht werden können. Die hiermit verbundenen Eingriffe (vor allem in die Berufsfreiheit) können lediglich dann gerechtfertigt sein, wenn die Verpflichtung zur Teilnahme an Selbstregulierungsmaßnahmen einem öffentlichen Interesse dient (in diesem Fall dem Schutz des informationellen Selbstbestimmungsrechts) und die zugrunde liegende gesetzliche Regelung angemessen ist.[707]

Selbstverpflichtungen wie z.B. der Kodex der Branche zu Geodatendiensten haben in der Regel eine weitere große Schwäche: Ihre rechtliche Bindungswirkung ist – jedenfalls im Außenverhältnis[708] – gering, weil sie den Betroffenen regelmäßig keine gerichtlich durchsetzbaren

---

[702] Teilweise wird indes bei Verhaltensregeln ein „datenschutzrechtlicher Mehrwert“ zu dem bereits durch Gesetz gewährleisteten Datenschutzniveaus gefordert, vgl. *Schaar*, DuD 2003, 421 (424).

[703] Vgl. hierzu oben D.II.1.d).

[704] *Weichert* in: Däubler/Klebe/Wedde/Weichert, § 3 Rn. 2.

[705] Eine Analyse, welche Verhaltenskodizes in anderen Wirtschaftsbereichen bestehen, erfolgt in dieser Arbeit nicht. Eine vertiefte Auseinandersetzung mit den Instrumentarien der Selbstregulierung bleibt anderen wissenschaftlichen Arbeiten vorbehalten. Für die Diskussion um RFID-Datenschutz ist die Möglichkeit der Selbstregulierung aber ein interessantes und künftig ggf. wichtig werdendes Instrument, weswegen die Arbeit in gebotenem Umfang darauf hinweist.

[706] *Schröder*, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, S. 172.

[707] Vgl. hierzu *Roßnagel* in: Roßnagel, HdB DSR, 3.6 Konzepte der Selbstregulierung, Rn. 20.

[708] Haftungen gegenüber dem Verband oder der sonstigen Vereinigung, die die Verhaltensregeln erstellt hat sind beispielsweise infolge der Implementierung der Verhaltensregeln in die Verbandssatzung möglich. Dies hat

Ansprüche vermitteln.[709] Verbindlichkeit mit der Möglichkeit der Durchsetzung erfahren Verhaltensregeln im Verhältnis zum Betroffenen aber dann, wenn sie – z.B. als AGB – in einen Vertrag mit dem Betroffenen aufgenommen werden.[710] Dies setzt aber natürlich voraus, dass der Abschluss eines Vertrages überhaupt von den beiden Parteien gewünscht und geplant ist. Bei Verhältnissen ohne vertragliche Verbindung scheidet eine solche Einbeziehung regelmäßig aus. Gleichfalls werden den Aufsichtsbehörden per Gesetz keine Befugnisse zur Überwachung der Einhaltung der verabschiedeten Verhaltensregeln oder gar Sanktionsmöglichkeiten eröffnet. Den Aufsichtsbehörden verbleibt auch bei Vorliegen von über den gesetzlichen Standard hinausgehenden Verhaltensregeln nur die Überwachung der Einhaltung der gesetzlichen Regelungen. Die Einhaltung der Verhaltensregeln bleibt damit ohne drohende Sanktionen seitens des Staates allein Sache der sie anwendenden Unternehmen.

In Bezug auf RFID würde auch die Bundesregierung es begrüßen, wenn die Wirtschaft eine Selbstverpflichtung zur Gewährleistung eines angemessenen Datenschutzniveaus in RFID-Anwendungen abschließen würde.[711] Ein Hintergrund ist sicher, dass gerade im Hinblick auf die Unterschiede bei RFID-Anwendungen spezialgesetzliche Regelungen schnell mit dem Ansatz der Technikneutralität im europäischen und deutschen Datenschutzrechts kollidieren würden.[712]

EPCglobal Inc.[713] hat bereits 2005 Richtlinien für die Verwendung von RFID-Tags mit dem Electronic Product Code (EPC) im Zusammenhang mit Konsumgütern verabschiedet.[714] Die Richtlinien sollen Anwender des EPC dabei unterstützen, die umfassenden nationalen und internationalen datenschutzrechtlichen Vorgaben einzuhalten, die an RFID-Systeme gestellt werden. Zwar haben die Richtlinien keinerlei Bindungswirkung – nicht einmal gegenüber EPCglobal besteht die Pflicht, sie einzuhalten – sie dienen aber als Beispiel dafür, wie eine Selbstverpflichtung der Wirtschaft aussehen könnte und sollen vor diesem Hintergrund hier vorgestellt werden.

Die Richtlinien basieren auf den Prinzipien der Verantwortlichkeit der Industrie, der Information der Konsumenten sowie dem Wahlrecht der Konsumenten und sollen kontinuierlich – angepasst an die Entwicklungen der Technik sowie der Anwendungen und den hieraus erwachsenden Herausforderungen – weiterentwickelt werden. Die Richtlinien umfassen die

---

allerdings für den einzelnen Betroffenen keine Wirkung. Vgl. hierzu *Schröder*, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, S. 174 ff.; *Abel*, RDV 2003, 11 (12).

[709] Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 204; Taeger/Gabel/*Kinast*, § 38a BDSG Rn. 18.

[710] Taeger/Gabel/*Kinast*, § 38a BDSG Rn. 35.

[711] S. u. E.III.

[712] Bundesministerium für Wirtschaft und Technologie, European Policy Outlook RFID, 2007, abrufbar unter http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeuropeancommision/European_Policy_Outlock_RFID.pdf (04.04.2013), S. 31.

[713] Vgl. hierzu oben C.I.1.

[714] GS1, Guidelines on EPC for Consumer Products, Stand September 2005, abrufbar unter http://www.gs1.org/epcglobal/public_policy/guidelines (04.04.2013).

Punkte „Information“, „Wahlrecht“, „Weiterbildung“ sowie „Verwendung, Speicherung und Sicherheit der Daten“.

Auf diesen (internationalen) Richtlinien aufbauend, hat *GS1 Germany*, die deutsche Vertretung von *EPCglobal*, gemeinsam mit der deutschen Wirtschaft ein Positionspapier „RFID Daten- und Verbraucherschutz“[715] erarbeitet, indem sie insgesamt sechs – nach ihrer Vorstellung – über die Vorgaben des Datenschutzrechts hinausgehende Grundsätze zur Verwendung von RFID-EPC in der Verbrauchersphäre formulieren[716]:

- *Information und Aufklärung*

  Hiermit sind allgemeine Informationen über RFID, EPC und entsprechende Anwendungen und Einsatzbereiche für den Verbraucher gemeint. Umfasst ist aber auch ein RFID-Warenlogo.

- *Verständlichkeit*

  Die bereitgestellten Informationen müssen in verständlicher Form und deutscher Sprache sein.

- *Kennzeichnung*

  Der Punkt der Warenkennzeichnung wird gesondert aufgenommen: Getaggte Verbrauchsgegenstände sollen mit einem von EPCglobal entwickelten Logo gekennzeichnet werden, um den Verbraucher auf die Verwendung von RFID-EPC zu informieren. Für weitergehende Informationen soll auf die Informationen unter Punkt 1 zurückgegriffen werden.

- *Deaktivierbarkeit*

  Dem Verbraucher soll die Möglichkeit eingeräumt werden, das Tag z.B. durch Entfernung zu deaktivieren.

- *Sicherheit*

  Die Möglichkeit der Auslesung der RFID-EPC Tags soll durch Entwicklung entsprechender Schutzmaßnahmen unterbunden werden.

- *Gewährleistung/Serviceabwicklung*

  Neben der Möglichkeit der Inanspruchnahme von Gewährleistungsrechten und Services mithilfe des RFID-EPC Tags auf dem erworbenen Verbrauchsgegenstand soll dem Kunden auch weiterhin die Möglichkeit verbleiben, statt dessen den Kassenbeleg vorzulegen, ohne dass ihm hierbei Nachteile erwachsen dürfen.

---

[715] GS1 Germany, RFID Daten- und Verbraucherschutz, Positionspapier der deutschen Wirtschaft, Stand Juni 2006, abrufbar unter http://www.gs1-germany.de/common/downloads/epc_rfid/3001_daten_verbraucherschutz.pdf (04.04.2013).

[716] GS1 Germany, RFID Daten- und Verbraucherschutz, Positionspapier der deutschen Wirtschaft, Stand Juni 2006, oben Fn. 715, S. 8 f.

Bei diesen – von GS1 Germany selbst Selbstverpflichtungserklärung genannten[717] – Richtlinien handelt es sich lediglich um ein unverbindliches Positionspapier. Die an seiner Entwicklung mitwirkenden Unternehmen haben sich nicht verpflichtet, diese Richtlinien auch zu befolgen. Deshalb fordert das Positionspapier

> „Unternehmen und Wirtschaftskreise, die entsprechende Anwendungen nutzen wollen, […] [auf], die aufgeführten Grundsätze für einen verantwortlichen Umgang mit RFID auf Basis des EPC in ihren unternehmenseigenen Verbraucherschutzrichtlinien aufzunehmen und zu veröffentlichen."[718]

Mit der Aufnahme in die unternehmenseigenen Verbraucherschutzrichtlinien könnte – werden diese als AGB Bestandteil des Vertrags mit dem Betroffenen – eine Bindungswirkung hergestellt werden. Diesseits ist allerdings nicht bekannt, dass eine solche Implementierung bis jetzt stattgefunden hat.

bb) Datenschutzaudit

Selbstregulierung ist auch durch die Durchführung von Datenschutzaudits und die Verleihung von Datenschutzgütesiegeln durch unabhängige Stellen möglich. Datenverarbeitende Stellen und Systemhersteller können ihre Produkte und Datenverarbeitungssysteme auf ihre Datenschutzverträglichkeit hin überprüfen und sich dies werbe- und damit wettbewerbswirksam zertifizieren lassen. Ein Zertifikat soll hierbei nicht erhalten, wer lediglich die gesetzlichen Regelungen einhält; die sich um ein Gütesiegel bewerbende Stelle soll vielmehr ein hierüber hinausgehendes Datenschutzniveau gewährleisten.[719] Zertifiziert werden können von daher auch Verhaltensregeln von Verbänden oder vergleichbaren Vereinigungen, wenn sie ein höheres Datenschutzniveau gewährleisten, als dies bereits durch das geltende Datenschutzrecht der Fall ist.

Das BDSG sieht die Durchführung solcher Datenschutzaudits bereits in § 9a vor:

> § 9a Datenschutzaudit
>
> Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

Das in § 9a S. 2 BDSG vorgesehene Datenschutzauditgesetz ist bis heute nicht verabschiedet worden. 2009 hatte die Bundesregierung zwar einen entsprechenden Gesetzentwurf[720] in den Bundestag eingebracht, dieser wurde allerdings vom federführenden Innenausschuss dahingehend abgeändert, dass die vorgesehenen Regelungen zum Datenschutzauditgesetz gestrichen

---

[717] http://www.gs1-germany.de/standards/epc_rfid/datenschutz/index_ger.html (04.04.2013).

[718] GS1 Germany, RFID Daten- und Verbraucherschutz, Positionspapier der deutschen Wirtschaft, Stand Juni 2006, oben Fn. 715, S. 3.

[719] Vgl. Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BTDrucks 16/12011 vom 18.02.2009, abrufbar unter http://dipbt.bundestag.de/dip21/btd/16/120/1612011.pdf (04.04.2013), S. 1.

[720] Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BTDrucks 16/12011 vom 18.02.2009, oben Fn. 719, S. 7 ff.

wurden[721]. Der Bericht des Innenausschusses sah vor, dass vor einer gesetzlichen Regelung zunächst ein dreijähriges Modellprojekt für eine Branche erfolgen sollte. Datenschutzaudits werden aber heute bereits durch unterschiedliche Stellen durchgeführt, so etwa durch das Unabhängige Landesdatenschutzzentrum Schleswig-Holstein (ULD)[722] oder den TÜV[723].

Im Koalitionsvertrag von 2009 haben sich die Regierungsparteien dazu verpflichtet, eine Stiftung Datenschutz zu errichten,

> „die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein **Datenschutzaudit** [Hervorhebung eingef. d. Verf.] zu entwickeln.“[724]

Die Stiftung ist bis jetzt nicht ins Leben gerufen worden. Für den Haushalt 2011 waren aber bereits 10 Millionen Euro hierfür eingeplant. Eine gesetzliche Grundlage soll hierfür nach momentanem Stand aber wohl auch weiterhin nicht geschaffen werden. Nach den Plänen der Regierung soll die Stiftung 2012 errichtet werden und neben die bereits bestehenden Zertifizierungsstellen treten.[725]

Mit der Auditierung und anschließenden Zertifizierung von RFID-Systemen und Systemkomponenten könnte ein wichtiger Schritt auf dem Weg zu mehr Akzeptanz gemacht werden. Zwingende Voraussetzung hierfür ist aber, dass auf die Spezifika der verschiedenen Systeme und Anwendungen durch Anpassung der Auditverfahren eingegangen wird und erkennbar wird, welche Prüfungen vorgenommen worden sind und wie eine positive Zertifizierungsentscheidung zu Stande kommt. Hierfür sind transparente und der Öffentlichkeit zugängliche Ausführungsbestimmungen zu schaffen. Hierbei dürfte es weniger darauf ankommen, dass der Gesetzgeber solche erlässt; auch die Zertifizierungsstelle selbst kann hiermit betraut werden. Wichtig ist, dass es überhaupt Maßstäbe gibt, an denen erkennbar wird, wie die Auditierung von Statten geht, um so eine Vergleichsmöglichkeit für die Betroffenen herzustellen.

b) RFID-Datenschutzfolgenabschätzung als Maßnahme der Selbstregulierung

Anders als vom BITKOM in seiner Pressemitteilung[726] dargestellt, handelt es sich bei dem Rahmen für Datenschutzfolgenabschätzung für RFID-Anwendungen nicht um eine Selbstverpflichtung i.S.v. Verhaltensregeln. Der Rahmen für Datenschutzfolgenabschätzungen ist auch in sonstiger Hinsicht – ebenso wie die Empfehlung selbst – kein verbindliches Dokument, aus

---

[721] Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss), BTDrucks 16/13657 vom 01.07.2009, abrufbar unter http://dipbt.bundestag.de/dip21/btd/16/136/1613657.pdf (04.04.2013), S. 2.

[722] Vgl. die Homepage des ULD https://www.datenschutzzentrum.de/audit/index.htm (04.04.2013).

[723] Vgl. die Homepage des TÜV Rheinland http://www.tuv.com/de/deutschland/gk/consulting_informationssicherheit/strategische_informationssicherheit/datenschutz_zertifizierung_unternehmen/datenschutz_zertifizierung_unternehmen.jsp?null (04.04.2013).

[724] Koalitionsvertrag CDU, CSU, FDP 2009, abrufbar unter http://www.cdu.de/doc/pdfc/091026-koalitionsvertrag-cducsu-fdp.pdf (04.04.2013), S. 106.

[725] So Jimmy Schulz, MdB (FDP) auf einer Veranstaltung der Schufa zum Datenschutz am 22.11.2011 in der Landesvertretung Rheinland-Pfalz.

[726] BITKOM Pressemittelung vom 06.04.2011, Selbstverpflichtung zum Datenschutz bei RFID, abrufbar unter http://www.bitkom.org/de/themen/50792_67587.aspx (04.04.2013).

dem sich durchsetzbare Pflichten für die Mitgliedstaaten oder die betroffenen Unternehmen ableiteten ließen.[727] Die Datenschutzfolgenabschätzung stellt vielmehr ein Werkzeug zur Risikoanalyse dar, aus der sich aber noch keine Pflicht der sie anwendenden Unternehmen ergibt, aus den Ergebnissen der Analyse bestimmte Verhaltensregeln abzuleiten und sich an diese zu halten. Sie soll als eine Art Bestandsaufnahme fungieren, die es den zuständigen Behörden ermöglichen soll, die betreffende RFID-Anwendung umfassend rechtlich zu bewerten. Nichts desto trotz handelt es sich um eine Maßnahme der Selbstregulierung, ist doch bereits die Feststellung datenschutzrechtlicher Risiken sowie die Auseinandersetzung mit möglichen technischen und organisatorischen Maßnahmen zur Minimierung dieser Risiken ein Bestandteil selbstverantworteten datenschutzfördernden Verhaltens. Scheitert dieses Konzept der Selbstregulierung, kann dies zu einem strengeren Regulierungsansatz führen.[728]

aa) Erster Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen

Der im März 2010 von der Branche vorgelegte Rahmen für Datenschutzfolgenabschätzungen in RFID-Anwendungen basiert auf einem Datenschutz- und Risikomanagementansatz und fokussiert die Umsetzung der RFID-Empfehlung sowie die Einhaltung europäischen Datenschutzrechts und bewährter Verfahren.[729]

Die Ziele der RFID-Datenschutzfolgenabschätzung sind[730]:

- die Identifizierung von Auswirkungen auf den Datenschutz durch die betreffende RFID-Anwendung, soweit gegeben, u.a. die Möglichkeit, den Einzelnen mithilfe der RFID-Anwendung zu überwachen;
- die Angabe, ob der Betreiber der RFID-Anwendung angemessene technische und organisatorische Maßnahmen, u.a. Kontrollen und Maßnahmen für Einzelne, getroffen hat, um den Schutz personenbezogener Daten und des informationellen Selbstbestimmungsrechts sicherzustellen;
- die Dokumentation der getroffenen technischen und organisatorischen Maßnahmen für den angemessenen Schutz personenbezogener Daten und des informationellen Selbstbestimmungsrechts, u.a. Maßnahmen zur Minimierung identifizierter Datenschutzauswirkungen sowie
- die Dokumentation der gesamten Analyse und des Ergebnisses in einem Datenschutzfolgenabschätzungsbericht, der den zuständigen Behörden, also den Datenschutzbehörden, übermittelt werden kann, bevor die Anwendung verwendet wird.

---

[727] Vgl. Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 4.

[728] Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 4.

[729] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 4.

[730] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 5.

Nach Einführung von Schlüsselbegriffen und ihrer Definition[731] nimmt die Branche eine Klassifizierung der Kriterien von RFID-Anwendungen vor. Sie unterscheidet vier datenschutzrechtlich unterschiedlich zu behandelnde Level[732]:

- Level 0: Die RFID-Anwendung verarbeitet keine personenbezogenen Daten. Die Informationen auf dem RFID-Tag beinhalten keine personenbezogenen Daten und getaggte Gegenstände sollen nur vom System-Betreiber besessen werden. Die RFID-Anwendung verknüpft die Informationen auf dem RFID-Tag nicht mit personenbezogenen Daten.
- Level 1: Die RFID-Anwendung verarbeitet keine personenbezogenen Daten. Getaggte Gegenstände in der RFID-Anwendung sollen von einzelnen Personen besessen werden. Das RFID-Tag beinhaltet jedoch keine personenbezogenen Daten und die RFID-Anwendung verknüpft die Informationen auf dem RFID-Tag nicht mit personenbezogenen Daten.
- Level 2: Die RFID-Anwendung verarbeitet personenbezogenen Daten. Die Informationen auf dem RFID-Tag beinhalten keine personenbezogenen Daten aber die Anwendung verknüpft nicht personenbezogene Informationen auf dem RFID-Tag mit Personen oder personenbezogenen Daten. Weitere Betrachtungen können nötig sein, wenn die Anwendung sensible personenbezogene Daten verarbeitet (z.B. medizinische oder biometrische Informationen).
- Level 3: Die RFID-Anwendung verarbeitet personenbezogene Daten und die Informationen auf dem RFID-Tag beinhalten personenbezogenen Daten. Weitere Betrachtungen können nötig sein, wenn die Anwendung sensible personenbezogene Daten verarbeitet (z.B. medizinische oder biometrische Informationen).

Im Rahmen einer ersten Analyse soll festgestellt werden, ob überhaupt eine Datenschutzfolgenabschätzung für die betreffende RFID-Anwendung erforderlich ist. Dies soll nach Ansicht der Branche bei Anwendungen, die als Level 0 eingestuft worden sind, nicht der Fall sein.[733] Anwendungen, die als Level 1 bis 3 eingestuft worden sind, sollen einer vierstufigen Analyse unterzogen werden. Der abschließende Bericht für die Datenschutzbehörden soll folgende Teile enthalten:

- Teil A: RFID-Anwendungsbeschreibung und RFID-Anwendungsbereich
- Teil B: RFID Steuerungsmechanismen
- Teil C: Verantwortlichkeit
- Teil D: Analyse und Entscheidung

[731] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 5.

[732] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 7.

[733] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 9.

In Teil A soll zunächst eine umfassende Bestandsaufnahme beinhaltend die technischen Eigenschaften der Anwendung, die verarbeiteten Daten, die mit den Daten in Verbindung tretenden Personen (unabhängig davon, ob sie identifiziert bzw. identifizierbar sind oder nicht) sowie die Verwender der Daten (Betreiber und Dritte) durchgeführt werden. Aufgenommen werden soll auch, ob personenbezogene Daten i.S.d. DSRL in den RFID-Tags enthalten sind oder ob die Tag-Daten mit personenbezogenen Daten, auf die der Betreiber oder Dritte Zugriff haben, verknüpft werden können.[734]

In Teil B sollen Datenschutz- und Datensicherheitsmaßnahmen adressiert werden, die in die RFID-Anwendung eingebaut sind, um potenzielle Risiken zu minimieren.[735]

In Teil C der individuellen Datenschutzfolgenabschätzung sollen die Verantwortlichkeitsstrukturen für die betreffende RFID-Anwendung dargestellt werden. Dies beinhaltet auch Regeln über Transparenz und die Information der Betroffenen über die Verwendung von RFID.[736]

Der letzte Teil D der Datenschutzfolgenabschätzung dient einer abschließenden Einschätzung, in der der Betreiber bestimmen soll, ob die Anwendung nach Auswertung der gesammelten Informationen mit geltendem Datenschutzrecht konform ist und damit eingeführt werden kann oder nicht. Der Abschlussbericht soll der zuständigen Datenschutzbehörde spätestens sechs Wochen vor der geplanten Einführung der Anwendung zur Prüfung vorgelegt werden.[737]

In ihrer Stellungnahme zu dem ersten Rahmen für die Datenschutzfolgenabschätzung äußert die Artikel-29-Datenschutzgruppe zu drei inhaltlichen Aspekten wesentliche Bedenken. Diese betreffen die Frage der Risikobewertung, von Personen mitgeführte RFID-Tags sowie den Einsatz von RFID im Einzelhandel.[738]

Die Datenschutzgruppe bemängelt, dass der doch eigentlich von der Datenschutzfolgenabschätzung verfolgte – und von der Branche auch erkannte – Aspekt der Aufdeckung und Bewertung etwaiger datenschutzrechtlicher Risiken im vorgelegten Rahmen fehlt.[739]

Erheblich fällt die Kritik der Gruppe zu der datenschutzrechtlichen Bewertung von produktbezogenen Identifikationsnummern auf getaggten Gegenständen aus. Die Datenschutzgruppe führt aus, dass auch solche Produktidentifikationsnummern benutzt werden können, um die betroffene Person mit der Zeit zu erkennen und somit „identifizierbar“ zu machen. Sie betont,

---

[734] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 10 ff.

[735] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 14 ff.

[736] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 17 f.

[737] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, oben Fn. 655, S. 18 f.

[738] Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 7 ff.

[739] Für den ganzen Absatz vgl. Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 7 f.

dass es auf die Kenntnisnahme der sozialen Identität einer Person nicht ankommt, um Daten als personenbezogene zu qualifizieren; folglich enthalte ein „RFID-Tag, das von einer Person mitgeführt wird und eine eindeutige Kennung enthält, per definitionem personenbezogene Daten".

Nach Ansicht der Datenschutzgruppe müssen RFID-Anwendungsbetreiber dazu aufgefordert werden, Datenschutzprobleme zu beurteilen, die auftreten können, wenn Einzelpersonen RFID-Tags täglich mit sich führen. Dies umfasse auch das Risiko einer unbefugten Überwachung außerhalb der Anwendung.[740]

Die Datenschutzgruppe weist auf die bereits in der Empfehlung hervorgehobenen Besonderheiten im Einzelhandel hin, bei dem es am Häufigsten dazu kommen wird, dass Einzelpersonen RFID-Tags mit sich führen. Sie bemängelt, dass die Branche die ausdrücklich von der Empfehlung vorgesehene standardmäßige Deaktivierung oder Entfernung der RFID-Tags am Verkaufsort keinen Eingang in den Rahmen gefunden hat und fordert sie auf, eine entsprechende Klarstellung vorzunehmen.[741]

bb) Befürworteter Vorschlag

In ihrem überarbeiteten zweiten Vorschlag für einen Rahmen für eine Datenschutzfolgenabschätzung in RFID-Anwendungen führt die Branche zunächst ergänzend die Unterscheidung zwischen vollständiger und eingeschränkter Datenschutzfolgenabschätzung ein. Nach dieser neuen Staffelung sollen die oben bezeichneten Level 0 und 1 sich dadurch unterscheiden, dass Einzelpersonen die produktbezogenen RFID-Tags wahrscheinlich bei sich führen (dann Level 1) oder nicht (dann Level 0). Lediglich dann, wenn auch lediglich produktbezogene RFID-Tags wahrscheinlich nicht von Einzelpersonen bei sich geführt werden, soll keine Datenschutzfolgenabschätzung notwendig sein. Für die Fälle der Level 1 Anwendungen soll nur eine eingeschränkte Datenschutzfolgenabschätzung erforderlich sein. Diese unterscheidet sich von der vollständigen dadurch, dass sie – aufgrund der geringeren zu erwartenden datenschutzrechtlichen Risiken – in Umfang und Detailtiefe sowohl bezogen auf die Untersuchung als auch den abschließenden Bericht eingeschränkt ist.[742] Wie diese Einschränkungen konkret aussehen sollen, ergibt sich nicht aus dem Rahmen.

Die zweite Phase der eigentlichen Datenschutzfolgenabschätzung soll künftig zusätzlich zu den bereits im ersten Vorschlag eingeführten Punkten die Identifikation und Auflistung der potenziellen Datenschutzrisiken in Bezug auf die betreffende RFID-Anwendung sowie die Wahrscheinlichkeit der Risikoverwirklichung und ihre Größenordnung beinhalten. Hierfür kann eine Liste potenzieller Risiken aus Anhang 3 zum Rahmen entnommen werden.[743]

---

[740] Für den ganzen Absatz vgl. Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 9, 11.

[741] Für den ganzen Absatz vgl. Artikel-29-Datenschutzgruppe, WP 175, oben Fn. 323, S. 10.

[742] Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 12.01.2011, oben Fn. 657, S. 6 ff.

[743] Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 12.01.2011, oben Fn. 657, S. 9.

In Bezug auf die Pflicht zur Deaktivierung bzw. Entfernung von RFID-Tags weist die Branche nunmehr ausdrücklich auf die Bestimmungen in der Empfehlung hin, betont jedoch auch, dass eine Deaktivierung oder Entfernung dann nicht erforderlich ist, wenn nach durchgeführter Datenschutzfolgenabschätzung feststeht, dass von den betreffenden RFID-Tags wahrscheinlich keine Gefahr für Privatsphäre oder den Schutz der personenbezogenen Daten des Betroffenen ausgeht (vgl. Punkt 12 der Empfehlung).[744] In weiteren Anlagen stellt die Branche Vorlagen für die in den Abschlussbericht aufzunehmenden Informationen zusammen, so eine Liste über die erforderlichen Informationen für die Beschreibung der RFID-Anwendung (Anlage1), eine Übersicht über die Datenschutzziele der DSRL (Anlage 2) sowie eine Liste mit Beispielen für Kontroll- und Sicherheitsmaßnahmen (Anlage 4).

Diesen geänderten Entwurf hat die Artikel-29-Datenschutzgruppe befürwortet, sie äußert aber auch an der neuen Version Kritik.[745] Die Datenschutzgruppe begrüßt zwar den Umstand, dass nach Vorschlag der Branche alle RFID-Anwendungen, in denen RFID-Tags von Personen mitgeführt werden, einer Datenschutzfolgenabschätzung unterzogen werden sollen.[746] Sie bemängelt indes erneut die Einstufung von produktbezogenen RFID-Tags mit Identifikationsnummern. Die Datenschutzgruppe betont nochmals, dass ihrer Auffassung nach solche produktbezogenen Identifikationsnummern als personenbezogene Daten zu qualifizieren sind, sofern sie von Personen mitgeführt werden.[747] Sie weist zudem darauf hin, dass die Gefahr des Tracking und der Profilbildung auch dann besteht, wenn der Betreiber der Anwendung bei Einführung des Systems solche Ziele überhaupt nicht verfolgt, weil immer noch Dritte die Tags für solche Zwecke missbrauchen können.[748]

4. "Privacy-by-Design" durch "Privacy Enhancing Technologies" (PETs)

Neben der Datenschutzfolgenabschätzung führt die Empfehlung einen weiteren Begriff ein, der künftig aller Voraussicht nach erhebliche Bedeutung erlangen wird. In Punkt 17 sowie Erwägungsgründen 6 und 14 der Empfehlung fordert die Kommission, dass im Zuge weitergehender Entwicklungsmaßnahmen im Bereich von RFID-Anwendungen schon frühzeitig der Grundsatz der eingebauten Sicherheit und Privatsphäre (*Privacy-by-Design*-Ansatz) berücksichtigt werden soll.

Das traditionelle Datenschutzrecht legt hierfür bereits den Grundstein: § 9 BDSG in Kombination mit der Anlage sowie Art. 17 DSRL sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen ergreifen muss, die einen der Art der Daten und den bei der Datenverarbeitung bestehenden Risiken angemessenen Schutz gewährleisten. Weiterhin hat die verantwortliche Stelle den Grundsatz der Daten-

[744] Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 12.01.2011, oben Fn. 657, S. 9 f.

[745] Artikel-29-Datenschutzgruppe, WP 180, oben Fn. 339, S. 7.

[746] Artikel-29-Datenschutzgruppe, WP 180, oben Fn. 339, S. 6.

[747] Artikel-29-Datenschutzgruppe, WP 180, oben Fn. 339, S. 5.

[748] Artikel-29-Datenschutzgruppe, WP 180, oben Fn. 339, S. 6.

sparsamkeit und Datenvermeidung zu berücksichtigen und wann immer möglich anonymisierte oder pseudonymisierte Daten zu verwenden.

Eben diese Ziele können durch Verwendung technischer Maßnahmen – „Technologien zum Schutz der Privatsphäre" bzw. „*Privacy Enhancing Technologies*" (PETs) – erreicht oder jedenfalls gefördert werden.[749]

PETs – als Oberbegriff für jedwede datenschutzfördernde Technik – können in RFID-Anwendungen insbesondere folgende Funktionen[750] übernehmen:

- Automatische Datenanonymisierung nach einer bestimmten Zeit,
- Verschlüsselungsanwendungen, die ein unrechtmäßiges Auslesen von Daten bei deren Übermittlung verhindern,
- Die Schaffung einer *Platform for Privacy Preferences* (P3P) – ein Instrument eigentlich gedacht für Internetanwendungen, die es Internetnutzern ermöglicht, Einblick in die Datenschutzpolitik von Webseitenbetreibern zu erlangen und ihre Datenschutzpräferenzen mit dieser zu vergleichen – zugeschnitten auf die Bedürfnisse in RFID-Anwendungen.

Im Folgenden sollen die wichtigsten Technologien vorgestellt und auf ihre praktische Verwendbarkeit überprüft werden. RFID-Anwendungen betreffend können drei schutzbedürftige Bereiche unterschieden werden:

- Schutz der Daten auf dem Tag,
- Schutz der Kommunikation zwischen Tag und Reader und
- Schutz der des Hintergrundsystems.

In diesen drei Bereichen ergeben sich unterschiedlichste Gefahren für Datenschutz und Datensicherheit,[751] an deren Eindämmung sowohl Systembetreiber als auch -nutzer ein – in vielen Fällen nicht deckungsgleiches – Interesse haben. Es muss gewährleistet werden, dass die Daten auf den Tags nicht von Unberechtigten ausgelesen oder verändert werden; Tags müssen fälschungssicher sein, um eine eindeutige Identifizierungsmöglichkeit zu garantieren; ein unbefugtes Deaktivieren ist zu verhindern; die Kommunikation zwischen Tag und Reader ebenso wie zwischen Reader und Hintergrundsystem muss abhörsicher sein.

Zu berücksichtigen ist, dass der Schutz des vom Betreiber verwendeten IT-Hintergrundsystems – des *Backends* – nicht mehr Teil von RFID-*IT-Security* ist und damit nicht von dieser Arbeit erfasst werden kann. Entsprechend bleiben sowohl der Schutz der Daten auf den externen Datenträgern des Betreibers als auch der Schutz des Übertragungsvorgangs der Daten vom Reader auf das Backend vorliegend unberücksichtigt. Die sich hier er-

[749] Vgl. Mitteilung der Kommission KOM(2007) 228 endgültig, oben Fn. 660, S. 3.

[750] Vgl. zu den Funktionen Mitteilung der Kommission KOM(2007) 228 endgültig, oben Fn. 660, S. 4.

[751] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 41 ff.

gebenden klassischen Risiken innerhalb von Computersystemen weisen keine Besonderheiten zu anderen Systemen auf und können insbesondere nicht mit RFID-IT-Sicherheitsmaßnahmen gelöst werden.

Bei der technischen Gewährleistung von Datenschutz kann generell unterschieden werden zwischen Anonymisierung und Pseudonymisierung durch Löschen bzw. Veränderung der auf dem Tag gespeicherten Daten oder durch Kontrolle des Zugriffs auf die Tag-Inhalte.[752] Eine generell anwendbare Sicherheitsarchitektur für RFID Systeme ist aufgrund der unterschiedlichsten Anwendungsmöglichkeiten und Datenschutz-Anforderungen allerdings kaum vorstellbar.

Die erste schwache Stelle im RFID System ist das Tag. Ist dieses nicht ausreichend gegen unbefugte Zugriffe geschützt, kann theoretisch jeder die auf ihm gespeicherten Daten mit einem Reader auslesen, löschen und verändern.[753] Dies tangiert einerseits die Interessen des Betreibers, der, um sich auf sein System verlassen zu können, auf die Integrität und Verfügbarkeit der Tag-Daten angewiesen ist. Aufgrund der Tracking-Problematik müssen die Tag-Daten zudem zum Schutze des informationellen Selbstbestimmungsrechts des Betroffenen gegen unbefugten Zugriff geschützt werden.

Der zweite Schwachpunkt im RFID-System ist die Kommunikation zwischen Tag und Reader. [754] Unbefugte Lauschangriffe können einerseits darauf gerichtet sein, direkt die auf dem Tag gespeicherten und von ihm gesendeten Informationen oder aber eventuelle Zugangsschlüssel mitzuhören, um dann immer wieder auch auf verschlüsselte Tags zugreifen zu können. Im Gegensatz zum direkten unbefugten Zugriff auf das Tag ist hier die räumliche Komponente besonders zu bedenken. Während bei einem gezielten Zugriff auf ein bestimmtes (passives) Tag in der Regel eine enge räumliche Nähe hergestellt werden muss, die schneller auffällig und damit schwerer herzustellen sein wird, kann beim Abhören insbesondere der vom Reader an das Tag gesendeten Informationen (also insbesondere erforderlicher Zugangsschlüssel) aufgrund der teilweise großen Sendereichweiten eine viel größere Distanz eingehalten werden.[755] „Lauscher“ sind damit schwerer zu erkennen und abzuwehren. Neben dem bloßen Abhören sind auch weitere Angriffe, wie Störung oder vollständige Blockierung des Lesevorgangs etc. denkbar.[756] Der Kommunikationsvorgang zwischen Tag und Reader muss also ebenso wie das Tag selbst geschützt werden.

Die zur Erreichung dieser Schutzzwecke verwendeten Technologien werden im Folgenden kurz dargestellt.

---

[752] *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S. 223.

[753] Vgl. hierzu Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 63 f.

[754] Vgl. hierzu Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 61.

[755] Vgl. zu den möglichen Entfernungen beim Abhören Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 55 f.

[756] Vgl. *Finkenzeller*, RFID-Handbuch, S. 240.

a) Kill-Command oder Zerstörung

Der *Kill-Command* ist kurz gesagt nichts anderes als die dauerhafte Deaktivierung des RFID-Tags.[757] Gemeint ist hierbei nicht die physische Zerstörung des Tags, sondern die Deaktivierung mittels entsprechenden softwaregestützten Befehls. Das Tag wird also nicht dauerhaft abgeschaltet, sondern lediglich umprogrammiert. Zwar kann es dann in seinem neuen umprogrammierten Zustand keine oder nur noch sehr eingeschränkt Daten senden. Ist der *Kill-Command* allerdings nicht irreversibel, also so programmiert, dass er rückgängig gemacht werden kann, verbleibt die Möglichkeit, das Tag später wieder zu aktivieren.

Um absolut sicherzustellen, dass ein Auslesen des Tags und eine Reaktivierung unmöglich ist, bleibt nur die physische Zerstörung. Sowohl mittels Durchtrennung der Antenne als auch durch Zerstörung des Chips ist dies zu erreichen.[758]

Trotz der Gefahr der Reaktivierung nur deaktivierter Tags existieren in der Praxis bis jetzt lediglich softwarebasierte *Kill-Commands*.[759] Dies birgt den weiteren Nachteil, dass die Deaktivierung ebenso wie der Lesevorgang unsichtbar für den Kunden abläuft. Überprüft werden kann sie nur, indem das getaggte Produkt an ein Lesegerät gehalten wird. Des Weiteren erforderte die flächendeckende Verwendung von *Kill-Commands* eine entsprechende Ausstattung der Geschäfte und sonstiger Einrichtungen verantwortlicher Stellen mit der erforderlichen Hardware, den *Kill-Stations*. Unberücksichtigt blieben mit der Zerstörung der Tags Lesevorgänge innerhalb der Räume des RFID-Anlagenbetreibers, weil – im Beispiel des Supermarktes – die Deaktivierung ohnehin erst kurz vor dem Ausgang der Räumlichkeiten stattfände. Ein In-Store Tracking und Profiling, wie unter C.II beschrieben, kann mithin auf diesem Wege nicht verhindert werden.

Sowohl durch die physische Zerstörung als auch die Deaktivierung würden zudem die bereits beschriebenen Vorteile von RFID für den Verbraucher abgeschnitten. Weder die Ersetzung der papiernen Kassenbons noch der smarte Kühlschrank oder die bessere Abfallbeseitigung sind ohne funktionierende Tags auf den Produkten denkbar. Bei Miet- oder Leihverhältnissen wäre der *Kill-Command* schlechterdings nicht zu verwenden. Bibliotheken, die mittels RFID die Ausleihe organisieren, sind darauf angewiesen, dass die Tags auch noch beim Zurückbringen des Buches funktionieren.

Der „ganz-oder-gar-nicht"-Ansatz des *Kill-Commands* oder gar der Zerstörung erscheint demnach in vielen Anwendungen weder aus Sicht der RFID-Systembetreiber noch aus der der Kunden wünschenswert. Die bei bloßer Abschaltung der Tags verbleibende Ungewissheit über die Dauerhaftigkeit der Deaktivierung trägt ohnehin nur in begrenztem Umfang zu einer Akzeptanzsteigerung auf Kundenseite bei. Die Zerstörung brächte zwar aus Datenschutzge-

---

[757] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S.223 ff.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 341 ff.

[758] Hier ist auch die Verwendung stark überhöhter Frequenzbereiche – insbesondere im Mikrowellenbereich – denkbar, was zu einer termischen Zerstörung der Tags führte. Vgl. *Finkenzeller*, RFID-Handbuch, S. 238.

[759] *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S. 224.

sichtspunkten – abgesehen von Tracking und Profiling durch den Systembetreiber selbst – höchste Sicherheit. Die Vorteile von RFID wären aber ebenso unwiederbringlich beseitigt.

b) Challenge-Response-Verfahren

Das *Challenge-Response*-Verfahren kann zur gegenseitigen Authentifizierung von Tag und Reader eingesetzt werden.[760] Hierfür schickt die jeweils die Authentifizierung vornehmende Komponente – im Fall der Sicherung der Tag-Integrität also das Tag – eine Zufallszahl an den Reader (*Challenge*), welcher dann die Zahl mit einem beiden Seiten bekannten Schlüssel verschlüsselt und zurücksendet (*Response*). Auf diese Weise wird sichergestellt, dass nur autorisierte Reader Zugriff auf das Tag erhalten.[761] Diese Methode erfordert allerdings, dass das Tag kryptographische Algorithmen ausführen und Zufallszahlen generieren kann. Nur leistungsfähige Tags mit Rechnereinheit können diese Aufgabe ausführen. Für einen flächendeckenden Einsatz auf Produktebene scheidet das Verfahren mithin aus Kostengründen aus.

c) Hash Locks und MetaIDs

Eine weitere Möglichkeit zur Gewährleistung der Tag-Integrität ist die Anonymisierung der RFID-Tags mittels MetaIDs.[762] Grundsätzlich geht es hierbei darum, dass der jeweils berechtigte Tag-Inhaber die Kontrolle hierüber hat. Mittels der Verwendung von „*hashes*“ verschließt der Besitzer das Tag, indem er einen beliebigen Schlüssel wählt, mit dem eine MetaID erstellt wird. Diese wird auf dem Tag gespeichert. Gerät ein solches „MetaID-Tag“ in den Sendebereich eines Readers, antwortet es nicht mehr mit seinem EPC oder sonstigen Daten, sondern nur noch mit der MetaID. Der Inhaber des hierzugehörigen Schlüssels kann diesen zurück an das Tag senden. Nachdem überprüft wurde, ob Schlüssel und MetaID zusammenpassen, wird letztere gelöscht und der Inhalt des Tags wieder frei gegeben. Der Vorteil der MetaID-Methode ist der geringe Kostenfaktor. Hash-Funktionen lassen sich vergleichsweise einfach in Tags implementieren, sodass ihre Verwendung auch bei niedrigpreisigen Produkten noch wirtschaftlich ist.

Nachteilig wirkt sich allerdings aus, dass trotz der Verschlüsselung der Tag Informationen weiterhin ein Tracking möglich ist. Die vom Tag gesendete MetaID lässt eine genaue Identifikation ebenso zu, wie der extra verschlüsselte EPC auf dem Tag. Da aber auf den allermeisten RFID-Tags lediglich eine Identifikationsnummer gespeichert ist, bringt die MetaID-Methode keine breitentaugliche Verbesserung für den Schutz des informationellen Selbstbestimmungsrechts. Lediglich dann, wenn weitergehende Informationen auf dem Tag gespeichert sind, lohnt sich die Verwendung von *Hash Locks* und MetaIDs.

---

[760] Vgl. *Finkenzeller*, RFID-Handbuch, S. 253 f.; Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 47, 49 f.

[761] Dieses System wird bspw. verwendet vom ExxonMobil Speedpass, vgl. *Garfinkel*, RFID Payments at ExxonMobil *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 180 f.

[762] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S. 225 f.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 343 f.

d) Variable MetaIDs

Ein die Schwächen normaler MetaIDs ausgleichender Ansatz ist die Verwendung variabler MetaIDs bzw. *Randomized Hash-Locks*.[763] Das normale *Hash-Lock*-Verfahren wird hierbei um einen Zufallsgenerator erweitert. Das verschlüsselte Tag antwortet bei jedem Leseversuch mit einer neuen, anhand des Zufallsgenerators generierten MetaID und einem neuen Hashwert. Anhand dieser beiden Parameter kann dann der Schlüsselinhaber wiederum die „wahre" ID des Tags ermitteln und es somit freischalten, ohne dass das Tag die gleiche ID zweimal sendet. Mit diesem System wird also nicht nur das unautorisierte Auslesen des Tags sondern auch dessen Tracking verhindert.

e) Distanz-basierte Zugriffskontrolle

Ein anderer Ansatzpunkt ist die Einteilung des Umkreises, in dem ein Tag senden kann, in verschiedene Berechtigungsbereiche. Dabei gilt: Je weiter der Reader vom Tag entfernt ist, desto eingeschränkter ist das Zugriffsrecht. Befindet sich der Reader also in einer großen Entfernung, sendet das Tag nur minimale Informationen wie seine Identifikationsnummer. Ist der Reader in unmittelbarer Nähe, gibt das Tag alle Informationen frei, je nachdem, was auf ihm gespeichert ist.[764] Schwierigkeiten ergeben sich bei der Messung der Entfernung.[765] Genau das führt auch dazu, dass das System in der Praxis nicht bestehen kann. Schließlich hängt alles von einer genauen Distanzmessung ab. Außerdem ist auch hier zu bedenken, dass die allermeisten Tags lediglich minimale Informationen, wie den EPC, gespeichert haben. Eine Aufteilung in Berechtigungs-Distanzen ist damit in den meisten Fällen sinnlos, weil das Tag ohnehin nur eine Information liefern kann. Insofern wird auch mit dieser Technik kein Lösungsansatz für die Tracking-Problematik geliefert.

f) Blocker Tags

Blocker Tags sind eine weitere vergleichsweise kostengünstige Methode, um einen unberechtigten Zugriff auf die von einer Person mitgeführten Tags zu verhindern.[766] Kurz gesagt funktioniert das Blocker Tag wie ein Störsender. Es sendet dauernd sowohl Nullen als auch Einsen aus, sodass ein in Reichweite befindlicher Reader vorgegaukelt bekommt, es befänden sich Millionen Tags im Umkreis. In dieser fingierten Masse an Tags können die echten Tags versteckt werden, weil ein Auffinden durch den Reader nahezu ausgeschlossen ist. Einfachste Lösung scheint es damit zu sein, jedem Betroffenen ein Blocker Tag auszuhändigen. Damit wären Datenschutzherausforderungen wohl größtenteils gelöst. Ein nicht mehr auffindbares

---

[763] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S. 226 ff.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 344 ff.

[764] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S.231 ff.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 347 f.

[765] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S.231 ff.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 347 f.

[766] Vgl. *Finkenzeller*, RFID-Handbuch, S. 241, 248; *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S.234 f.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 350 f.; *Juels*, Technological Approaches to the RFID Privacy Problem" *in*: Garfinkel/Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy, S. 332 ff.

Tag kann auch nicht verfolgt werden. Die Tracking- und Profiling-Gefahr wäre damit gebannt. Allerdings führte die flächendeckende Verwendung solcher Blocker Tags dazu, dass auch alle gewünschten Anwendungen, die auf RFID basieren, gestört oder schlimmstenfalls sogar unmöglich gemacht würden. Eine Inventur mittels mobiler Lesegeräte wird unmöglich, wenn der Lagerarbeiter vergessen hat sein Blocker Tag abzulegen. Ein RFID „Türschlüssel" macht keinen Sinn, wenn der Inhaber gleichfalls sein Blocker Tag am Schlüsselbund trägt. Auch Blocker Tags liefern damit jedenfalls in ubiquitärer Verwendung keine optimale Lösung für einen datenschutzverträglichen Umgang mit RFID.

Hinzukommend ist gerade bei der möglichen Verwendung von Blocker Tags das vermutete Risiko der krebserregenden Wirkung von RFID zu berücksichtigen.[767] Aber auch ohne bewiesenes Krebsrisiko ist fraglich, inwieweit sich der Einzelne ständig weiteren elektromagnetischen Feldern aussetzten müssen soll, um ein Mindestmaß an Datenschutz zu erreichen.

g) Antikollisionsprotokolle

Ein Lesevorgang zwischen Reader und Tag erfolgt immer nach einem wiederkehrenden Muster: Der Reader sendet elektromagnetische Wellen aus, mittels derer die im Umkreis vorhandenen Tags aktiviert werden und ihre Antwort an den Reader zurücksenden. Um ein spezielles Tag zu identifizieren, verwenden Reader Antikollisionsprotokolle.[768] Dies funktioniert darüber, dass jedes Tag über einen einzigartigen binären Code aus Nullen und Einsen – einem ID-Präfix – sich von allen anderen unterscheidet. Um ein Tag mit dem Präfix „01100101" zu finden, sendet der Reader zunächst eine „0". Befinden sich in Lesereichweite mehr als nur ein Tag, deren Präfixe mit „0" beginnen, antworten auch all diese. Es kommt zu einer Kollision. Der Reader sendet daher die nächste Ziffer des Präfix, also eine „1". Dies führt er solange fort, bis er nur noch von einem – dem gesuchten – Tag Antwort erhält.

Bei diesem Vereinzelungsprozess stellt sich das Problem des Abhörens der Kommunikation von Reader zu Tag. Der Reader sendet in der Regel mit einer erhöhten Sendeleistung, damit er Tags in weiteren Umkreisen erreicht. Das führt dazu, dass die von ihm gesendeten ID-Präfixe aus größerer Entfernung mitgehört werden können. Bei Tags mit fortlaufenden Seriennummern wären dies in der Regel die kompletten IDs.[769] Mit diesen gewonnen Informationen könnte sich ein Angreifer Zugriff auf die Tags verschaffen. Um dies zu verhindern besteht die Möglichkeit den Lesevorgang mit den bereits vorgestellten Methoden abhörsicher zu machen. Eine Alternative ist, die Information, die der Reader an die Tags sendet, so zu reduzieren, dass ein Angreifer mit ihnen nichts anfangen kann. Sendet der Reader lediglich den Befehl: „Sende nächstes Bit der Präfix", auf den die Tags entsprechend antworten, weiß der

---

[767] Heise News Meldung vom 11.09.2007, Krebsverdacht bei implantierten RFID-Chips, abrufbar unter http://www.heise.de/newsticker/Krebsverdacht-bei-implantierten-RFID-Chips--/meldung/95797 (04.04.2013).

[768] Vgl. *Finkenzeller*, RFID-Handbuch, S. 220 ff.; *Langheinrich*, Personal Privacy in Ubiquitous Computing – Tools and System Support, S. 230 f.; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 348 ff.; auch *Gillert/Hansen*, RFID for the Optimization of Business Processes, S. 175.

[769] *Langheinrich*, Die Privatsphäre im Ubiquitous Computing *in*: Fleisch/Mattern, Das Internet der Dinge, S. 349.

Mithörende nicht, welche Präfixe ausgetauscht werden.[770] Der Reader kann dennoch durch Auswahl das richtige Tag finden. Nachteilig ist hierbei allerdings, dass Tags für diese Zwecke mit einem dynamischen Speicher ausgerüstet werden müssten, was die Kosten in die Höhe treiben würde.

Daher arbeitet die aktuelle Auto-ID/EPCglobal-Tag-Spezifikation mit einer Kombination aus MetaID und Antikollisionsprotokoll. Beim Anfragen der Präfixe durch den Reader senden die Tags nicht ihre wahre ID sondern lediglich die aufgesetzte und zufällig generierte MetaID. Damit kann das gesuchte Tag genauso gut gefunden werden, die auf ihm gespeicherten Informationen sind aber wiederum nur dem Schlüsselinhaber zugänglich.

h) Datenminimierung

Von der Zielrichtung von Abhörattacken ausgehend, dass entweder gleich der gesendete Tag-Inhalt oder zumindest der für den Zugriff erforderliche Schlüssel mitgehört wird, bietet es sich an, die auf dem Tag gespeicherten Informationen so gering zu halten, dass ein Mithören für den Angreifer sinnlos wird.[771] Dies ist dann der Fall, wenn es dem Angreifer darauf ankommt, die Tag-Daten oder die Informationen, die es repräsentiert, in Erfahrung zu bringen. Ist auf dem Tag lediglich die Identifikationsnummer gespeichert und muss für alles Weitere auf das Hintergrundsystem zugegriffen werden, liefen Abhörmaßnahmen in vielen Fällen leer. Nicht verhindert werden kann damit allerdings wie gesehen das Tracking von einzelnen Personen. Eine bloße Minimierung der Tag-Daten ohne weitergehende Sicherungsmaßnahmen ist damit nicht ausreichend.

i) RFID-"Platform for Privacy Preferences" (P3P)

Die bis jetzt dargestellten technischen Maßnahmen zielen alle auf den Schutz der Daten vor Auslese- oder Mithörversuchen unberechtigter Dritter ab. Nicht geschützt wird der Betroffene – außer bei Verwendung eines Blocker-Tags – indes vor Tracking- und Profilingversuchen seitens der Tag ausgebenden Stelle.

Die Verwendung einer *Platform for Privacy Preferences* (P3P) als ein Bauteil des *Electronic Identity Managements* – elektronisches Identitätsmanagement (eIDM) würde den Betroffenen dazu ermächtigen selbst durch Voreinstellungen zum gewünschten Datenschutzniveau zu bestimmen, welche Auslesevorgänge erfolgreich sein und welche abgewehrt werden sollen.

Der Begriff der *Platform for Privacy Preferences* (P3P) wurde vom World Wide Web Consortium (W3C) für in die Internetinfrastruktur implementierte Datenschutzstandards entwickelt. Mithilfe des mittlerweile in eine Reihe von Browsern integrierten Werkzeugs können Nutzer vorab selbst einstellen, welche Datenschutzstandards von ihnen angesurfte Websites erfüllen müssen, um eine Verbindung zu erlauben. Dies geschieht durch einen Abgleich der Voreinstellungen mit den – von den Betreibern getroffenen – Angaben auf der Website. Er-

[770] So genanntes „Silent Tree-Walking", vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 51.

[771] Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen", oben Fn. 83, S. 50.

füllt die angesurfte Website die gewünschten Standards, wird eine Verbindung hergestellt, andernfalls nicht. Durch diese technisierten Voreinstellungen erübrigt sich das Durchlesen verschiedener Datenschutzbestimmungen verschiedener Seitenbetreiber: P3P automatisiert diesen Vorgang.[772]

Ähnlich könnte auch ein Modell für RFID-Systeme aussehen: Auf Basis von Protokollen aufbauend auf die oben genannten Verfahren können Parameter festgelegt werden, nach denen ein Auslesen ermöglicht oder verhindert wird. Diese Parameter könnten z.B. Beschränkungen der Datensammlung, Zwecknennung, Transparenz und Verantwortlichkeit festlegen.[773] Mithilfe einer eindeutigen *Reader-Policy-ID* (RPID) könnte eine gegenseitige Identifikation zwischen RFID-Tag und RFID-Reader ermöglicht werden. Im Anschluss an diese Identifikation könnte – über einen separaten Informationskanal – dann die Datenschutzpolicy der den Reader betreibenden verantwortlichen Stelle z.B. auf das Smartphone des Betroffenen geladen werden. Das Smartphone (vgl. zu NFC-tauglichen Smartphones bereits oben B.I.2.b)dd)) könnte gleichfalls als „Wächter-Tag" fungieren, das alle Auslesevorgänge sichtbar macht, sodass jeweils die zugehörigen Datenschutzregeln sichtbar gemacht und protokolliert werden können.[774] Ein solches Verfahren hätte gegenüber dem Einsatz von Hinweisen auf Produkten und Readern mittels Kennzeichen den Vorteil, dass die Entscheidung, welche Auslesevorgänge erlaubt sein sollen und welche nicht, automatisiert würden, der Betroffene also nicht jedes Mal aktiv werden muss, um das von ihm angestrebte Schutzniveau zu erreichen.

Solange allerdings nicht verbindlich – per Gesetz – vorgegeben ist, dass die Betreiber von RFID-Systemen entsprechende Protokolle verwenden müssen und die dort angegebenen Datenschutzparameter auch auf ihre Richtigkeit überprüfbar sind, leidet die Verwendung von RFID-Datenschutzprotokollen an den gleichen Schwächen, wie P3P im Internet: Das System ist vollständig abhängig von der Offenheit und Ehrlichkeit der Systembetreiber. Ein nachhaltiger Schutz der Betroffenen kann dementsprechend nicht garantiert werden.[775]

III. Deutschland

Am 18 März 2011 hat der Bundesrat eine Entschließung veröffentlicht, in der er die Bundesregierung dazu auffordert, die Empfehlung der EU-Kommission umzusetzen und zu konkretisieren.[776] Die Entschließung geht auf einen Antrag des Landes Rheinland-Pfalz[777] zurück, der das Ergebnis eines zweijährigen Verbraucherdialogs in Rheinland-Pfalz darstellt[778].

---

[772] Vgl. die Homepage des P3P Projekts http://www.w3.org/P3P/ (04.04.2013).

[773] Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 283.

[774] Vgl. Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 283 f.

[775] Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, oben Fn. 78, S. 284.

[776] Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 18.03.2011, abrufbar unter http://www.bundesrat.de/cln_228/SharedDocs/Drucksachen/2011/0001-0100/48-11_28B_29,templateId=raw,property=publicationFile.pdf/48-11%28B%29.pdf (04.04.2013).

Die Entschließung ist seit Jahren der erste konkrete Vorstoß in Deutschland, sich dem Themenkreis RFID und Datenschutz wieder gesetzgeberisch zu nähern. 2008 hatte die Bundesregierung eine Unterrichtung „zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie“[779] veröffentlicht, in der sie sich dafür aussprach, zunächst abzuwarten, ob die aus RFID-Anwendungen erwachsenden Anforderungen an den Datenschutz durch eine zeitnah von der Wirtschaft abzuschließenden Selbstverpflichtung gewahrt werden. Erst in zweiter Linie sollten gesetzgeberische Maßnahmen erörtert werden.[780] Zuvor hatte die Bundesregierung bereits 2004 auf eine kleine Anfrage der FDP-Fraktion[781] offiziell Stellung zu der Frage genommen, ob gesetzgeberische Tätigkeiten in Bezug auf RFID erforderlich und zu erwarten sind. Dies hat sie damals verneint.[782] 2008 hatte die FDP-Fraktion zudem einen Antrag an den Deutschen Bundestag gestellt, indem sie forderte, dass der Verbraucherschutz und Transparenz bei RFID-Anwendungen gewährleistet werden solle.[783] Hierzu solle der Bundestag die Bundesregierung auffordern, einen Gesetzentwurf vorzulegen, der zum einen eine Deaktivierungs- bzw. Entfernungspflicht für RFID-Tags auf Einzelhandelsprodukten noch innerhalb der Geschäftsräume des RFID-Systembetreibers sowie eine transparente Gestaltung und Kennzeichnung aller Auslesevorgänge vorsieht, zum anderen den Betreiber von RFID-Systemen zur Implementierung von Sicherungsmechanismen gegen unbefugtes Auslesen zu verpflichten.[784] Der Antrag blieb unberücksichtigt.

Zuletzt hat die Bundesregierung erneut in Beantwortung einer kleinen Anfrage der Grünen-Fraktion[785] Stellung zu der Frage genommen, warum sie noch keine Maßnahmen zur Verbes-

---

[777] Antrag des Landes Rheinland-Pfalz, Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 03.02.2011, abrufbar unter http://www.bundesrat.de/cln_161/SharedDocs/Drucksachen/2011/0001-0100/48-11%2CtemplateId%3Draw%2Cproperty%3DpublicationFile.pdf/48-11.pdf (04.04.2013).

[778] Vgl. die Homepage des Landes Rheinland-Pfalz http://www.mulewf.rlp.de/service/topthemen-archiv/einzelansicht/archive/2010/september/article/conrad-und-wagner-funktechnologie-rfid-braucht-kennzeich-nung-und-transparenz-broschuere-inf-1/?print=1&cHash=0dec3d0d8e3e8591cd09374f625a9682 (04.04.2013).

[779] Unterrichtung durch die Bundesregierung, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie, oben Fn. 43.

[780] Unterrichtung durch die Bundesregierung, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie, oben Fn. 43, S. 15.

[781] Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP – Drucksache 15/3025 – Technologie der Radio Frequency Identification, BTDrucks 15/3190 vom 26.05.2004, oben Fn. 556.

[782] Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP – Drucksache 15/3025 – Technologie der Radio Frequency Identification, BTDrucks 15/3190 vom 26.05.2004, oben Fn. 556S. 3.

[783] Antrag der Fraktion der FDP, Datenschutz im nicht öffentlichen Bereich verbessern, BTDrucks 16/9452 vom 04.06.2008, abrufbar unter http://dip21.bundestag.de/dip21/btd/16/094/1609452.pdf (04.04.2013).

[784] Antrag der Fraktion der FDP, Datenschutz im nicht öffentlichen Bereich verbessern, BTDrucks 16/9452 vom 04.06.2008, oben Fn. 783, S. 6.

[785] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Nicole Maisch, Dr. Konstantin von Notz, Markus Tressel, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache

serung des Schutzes persönlicher Verbraucherdaten und zur Regulierung des Umganges unter anderem mit Funketiketten (RFID) oder Kundenprofilen vorgelegt hat. Auch zum jetzigen Zeitpunkt verweist die Bundesregierung auf die Möglichkeit, ein angemessenes Datenschutzniveau durch Selbstverpflichtungen der Wirtschaft zu erreichen, bevor gesetzgeberische Maßnahmen in Betracht zu ziehen sind.[786]

Eine solche Selbstverpflichtung ist für RFID-Anwendungen bis heute nicht von der Wirtschaft abgeschlossen worden. Hierauf weist auch der Bundesrat hin.

Vor diesem Hintergrund formuliert der Bundesrat konkrete Handlungsaufforderungen an die Bundesregierung, sollte die erstrebte Selbstverpflichtung nicht in naher Zukunft von der Wirtschaft umgesetzt werden:

> „Der Einsatz von RFID-Anwendungen in verbraucherrelevanten Bereichen soll mit einem Datenschutzkonzept verbunden sein, um die Sicherheit der persönlichen Daten zu gewährleisten.
>
> Die Verbraucherinformation sollte besonders dort, wo RFID zum Einsatz kommt, verstärkt werden.
>
> Die Kennzeichnung von RFID sollte nach international – zumindest europaweit – einheitlichen Standards erfolgen und leicht identifizierbar sein. Für RFID-Anwendungen im Einzelhandel sollte dabei neben einer Bereichskennzeichnung in Erwägung gezogen werden, einen produktbezogenen Hinweis auf RFID einzuführen, der sich am Produkt selbst befindet oder Teil der Produktkennzeichnung ist - also beispielsweise auf dem Etikett, am Regal, im Vertrag oder auf der Verpackung angebracht ist. Die Kennzeichnung von mit RFID-Chips versehenen Produkten in verbraucherrelevanten Bereichen auch außerhalb des Einzelhandels ist in diesem Zusammenhang ebenfalls zu prüfen.
>
> Eine Deaktivierung der Chips sollte auf einfachem Weg möglich und für alle Verbraucherinnen und Verbraucher nachvollziehbar sein.“ [787]

Die vorrangig angestrebte Selbstverpflichtung sollte insbesondere Vorgaben für die Kennzeichnung, Verbraucherinformation, für Datenschutzkonzepte und die Deaktivierung der RFID-Tags in verbraucherrelevanten Bereichen regeln.[788]

Sowohl neue gesetzliche Regelungen als auch eine etwaige Selbstverpflichtung der Wirtschaft dürften – das betont der Bundesrat – nicht dazu führen, dass die Anforderungen an die Wirksamkeit von datenschutzrechtlichen Einwilligungen abgesenkt oder aber dass Eingriffe in den unantastbaren Bereich des Persönlichkeitsrechts gerechtfertigt würden.[789] Der Bundesrat sieht in diesem Zusammenhang die Gefahr, dass sich einzelne Unternehmen mittels häufig als „Datenschutzerklärung“ getarnten Einwilligungserklärungen die Möglichkeit zur Erstellung von Kunden- und Persönlichkeitsprofilen verschaffen könnten, weswegen auch in Zukunft die

---

17/6797 – Erfüllung des Koalitionsvertrags und von Ankündigungen der Bundesregierung im Hinblick auf verbraucherpolitische Vorhaben, BTDrucks. 17/6881vom 01. 09. 2011, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/068/1706881.pdf (04.04.2013).

[786] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Nicole Maisch, Dr. Konstantin von Notz, Markus Tressel, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/6797 – Erfüllung des Koalitionsvertrags und von Ankündigungen der Bundesregierung im Hinblick auf verbraucherpolitische Vorhaben, BTDrucks. 17/6881vom 01.09.2011, oben Fn. 785, S. 13 f.

[787] Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 18.03.2011, oben Fn. 776, S. 1 f.

[788] Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 18.03.2011, oben Fn. 776, S. 6.

[789] Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 18.03.2011, oben Fn. 776, S. 2.

hohen Anforderungen an die Wirksamkeit datenschutzrechtlicher Einwilligungserklärungen nach § 4a BDSG eingehalten werden müssten.[790]

All diese Entwicklungen auf deutscher Ebene sind bis jetzt lediglich unverbindliche Wegweiser. In Anbetracht der Tatsache, dass die EU-Kommission bereits einen Entwurf für eine kohärente EU-Datenschutzgrundverordnung sowie für eine neue Datenschutzrichtlinie vorgelegt hat[791], die umfassende Regelungen für einen harmonisierten datenschutzrechtlichen Rahmen in der EU schaffen sollen, ist nicht zu erwarten, dass die Bundesregierung in nächster Zukunft im Bereich spezialgesetzlicher Regelungen zu RFID tätig wird.

IV. USA

In den USA ist der Begriff des Datenschutzes (*data protection*) eher unbekannt. Vielmehr wird auf das Konzept der *privacy* abgestellt. Die zwei Begriffe scheinen auf den ersten Blick inhaltlich identisch, sind es aber wohl nicht. Während *data protection* eine Gesamtheit von Maßnahmen (rechtlich und nicht-rechtlich) beschreibt, die darauf abzielt den Einzelnen vor ihn beeinträchtigenden Datenverarbeitungsmaßnahmen zu schützen und gleichzeitig bestimmte Prinzipien zur Datenverarbeitung beinhaltet, ist das Konzept der *privacy* ein breiteres. Dieses umfasst auch Aspekte wie den Schutz des persönlichen Raumes (Privat- und Familienleben, physische und moralische Integrität, Ehre und Ansehen, Schutz vor falscher Darstellung, Nichtveröffentlichung irrelevanter und verunglimpfender Fakten, unerlaubte Veröffentlichung privater Fotos, Schutz vor unberechtigter Verwendung privater Kommunikation, Schutz vor Veröffentlich vertraulich geäußerter oder erlangter Informationen).[792]

Die USA haben – anders als die EU – einen spezifischen und nur in engem Rahmen anwendbaren Ansatz im Hinblick auf Datenschutz gewählt.[793] Statt eines generellen Gesetzes als Rahmen für unterschiedlichste datenschutzrechtlich relevante Tatbestände haben die USA sowohl auf Bundes- als auch auf Staatenebene ein umfängliches Portfolio an Datenschutzspezialgesetzen erlassen.[794] Traditionelles U.S.-Datenschutzrecht – sowohl *tort* als auch *statutory law* – ist hierbei in seiner momentanen Form nicht auf RFID-Anwendungen anwendbar. Nichts desto trotz garantiert die U.S. amerikanische Verfassung ein Recht auf Privatheit (*right to privacy*).[795]

---

[790] Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 18.03.2011, oben Fn. 776, S. 6.

[791] Vgl. hierzu oben D.I.2.a)cc).

[792] Vgl. zum ganzen Absatz *Kuner*, European Data Protection Law, S. 3.

[793] *Stratford/Stratford*, Data Protection and Privacy in the United States and Europe, http://www.iassistdata.org/downloads/iqvol223stratford.pdf (04.04.2013).

[794] Einen Überblick über die existierenden US-Datenschutzgesetze bieten *Solove/Schwartz*, Information Privacy Law, S. 36 ff.; *Solove*, Digital Person: Technology and Privacy in the Information Age, S. 67 ff.;

[795] *Solove/Schwartz*, Information Privacy Law, S. 33; *Solove*, Digital Person: Technology and Privacy in the Information Age, S. 64 f.

Nach der Rechtsprechung des U.S. Supreme Court ergibt sich der Schutz der *privacy* aus einer Kombination des vierten und fünften Anhangs (*amendment*) zur U.S.-Verfassung.[796] Der vierte Anhang schützt den Einzelnen vor unrechtmäßigen Durchsuchungen und Beschlagnahmen und garantiert damit den Schutz der Privatheit und Würde gegen unberechtigte Eingriffe durch den Staat.[797] Der fünfte Anhang garantiert u.a. das Recht, sich nicht selbst belasten zu müssen. Wie alle verfassungsrechtlich garantierten Rechte schützen auch der vierte und fünfte Anhang zur U.S.-Verfassung den Einzelnen nur gegen Eingriffe des Staates. Sie gewähren hingegen – ebenso wie die deutschen Grundrechte – keinen unmittelbaren Schutz vor unberechtigter Erhebung und Verarbeitung personenbezogener Daten durch Private.[798]

Um in RFID-Anwendungen den erforderlichen Schutz der *privacy* auch im Verhältnis zu Privaten zu gewährleisten sind bereits diverse Gesetzgebungsverfahren – sowohl auf Bundes- als auch auf Staatenebene – zur Schaffung spezifischer RFID-Gesetze initiiert und durchgeführt worden. Insbesondere auf Staatenebene hat es diverse Ansätze gegeben, wie man RFID gesetzlich regeln könnte. Von den diskutierten Gesetzesentwürfen sind schlussendlich indes nur wenige verabschiedet worden.

1. Nationale Ebene

Bis jetzt wurde nur ein Versuch auf Bundesebene unternommen, ein spezielles RFID-Datenschutzgesetz einzuführen. Gesetzentwurf 2004 H.R.[799] 4673 "The Opt Out of ID Chips Act of 2004[800]" ist allerdings nie verabschiedet worden. Im Kern sollte das Gesetz den Einzelhandel dazu verpflichten, alle mit RFID getaggten Produkte entsprechend zu kennzeichnen (*labeling*) und den Kunden die Möglichkeit einzuräumen, an bzw. nach der Kasse (*point of sale* – POS) die Tags entfernt bzw. dauerhaft deaktiviert zu bekommen. Die Kennzeichnung sollte mindestens Informationen über das Vorhandensein von RFID-Tags und die Tatsache, dass diese dazu verwendet werden können, das Produkt zu verfolgen sowie dass die Tags eine einzigartige Identifikationsdaten an unabhängige Lesegeräte sowohl vor als auch nach dem POS übermitteln können. Darüber hinaus sollte es die Kunden über ihr Recht auf Entfernung oder Deaktivierung der Tags hinweisen. Die Kennzeichnung sollte entsprechend auffällig gestaltet und angebracht sein.

Der Gesetzentwurf beinhaltete zwei regulatorische Instrumente: Zum einen Information und zum anderen Entfernung oder Zerstörung/Deaktivierung. Diese zwei und weitere Elemente finden sich auch in Gesetzesinitiativen auf Staatenebene (hierzu sogleich).

---

[796] *Solove*, Digital Person: Technology and Privacy in the Information Age, S. 63.

[797] U.S. Supreme Court, Schmerber vs. California, 384 U.S., 757, 767 (1966).

[798] *Solove*, Digital Person: Technology and Privacy in the Information Age, S. 64.

[799] H.R. steht für „House of Representatives" – das U.S. Abgeordnetenhaus.

[800] 2004 Opt Out of ID Chips Act (Introduced in House), H.R. 4673 ICH (108th Congress), veröffentlicht auf der offiziellen Website der Bibliothek des U.S. Kongresses, abrufbar unter http://thomas.loc.gov/.

Abgesehen von diesem speziellen RFID-Datenschutzansatz finden sich U.S. bundesgesetzliche Regelungen zur Verwendung von RFID auch noch in Gesetzgebungen zur Medikamentenidentifikation[801] und zum neuen Führerschein (*enhanced driver's license*)[802].

2. Staatenebene

Die Gesetzgeber auf U.S.-Staatenebene sind und waren sehr viel aktiver und ausdauernder im Hinblick auf RFID-Datenschutzgesetzgebung als der Bundesgesetzgeber. Es haben sich unterschiedliche Kategorien[803] an Gesetzen herausgebildet, die alle unter den Oberbegriff RFID-Datenschutzrecht[804] gefasst werden können:

(a) Transparenzgesetzgebung (*Right-to-Know*)
(b) Verbotsgesetzgebung (*Prohibition*) und
(c) IT-Sicherheitsgesetzgebung (*IT-Security*).

a) Transparenzgesetzgebung

Transparenzgesetzgebung fordert im Kern Informationspflichten für die Betreiber von RFID-Systemen, besonders im Einzelhandel aber auch im Hinblick auf RFID-getaggte Identifikationsdokumente. Ziel entsprechender Gesetze ist, die Kunden bzw. Betroffenen darüber zu informieren, dass RFID-Technik Verwendung findet und welche die möglichen Gefahren für das Recht auf Privatheit sind.

Der oben angesprochene „Opt Out of ID Chips"-Ansatz auf Bundesebene stellt ein Beispiel für Transparenzgesetzgebung dar. In der Rechtsgeschichte finden sich vergleichbare Gesetzentwürfe[805] in 14 unterschiedlichen U.S. Bundesstaaten[806]: Alaska (2007 H.B. 421 und S.B. 293), Kalifornien (2007 S.B. 388), Massachusetts (2007 S.B. 159 und H.B. 261, 2009 S.B. 142), Minnesota (2009 H.B. 928, 1005, S.B. 345 und 1455), Missouri (2007 S.B. 13 und 210), Montana (2009 S.B. 154), New Hampshire (2007 H.B. 686, 2009 H.B. 478), New Jersey (2007 A.B. 3996, 2008 A.B. 1760), New York (2007 A.B. 222 und 261, 2009 A.B. 274 und

---

[801] Public Law 110-85, Sec. 505d "Pharmaceutical Security" Sub. Sec. (b) (3), vom 27.09.2007, 121 Stat. 823, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ085.110.pdf (04.04.2013).

[802] "RealID Act of 2005" (H.R. 418, 2005), später Title II des "Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005" (H.R. 1268, 2005).

[803] Vgl. zu den verschiedenen Kategorien an RFID-Gesetzgebung *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 207 ff.; ähnliche Kategorisierung auch bei *Schmid*, RFID Law in a Global Perspective *in*: Gillert/Hansen, RFID for the Optimization of Business Processes, S. 215 f.

[804] Vgl. *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 207 ff.

[805] H.B. steht für "House (of Representatives) Bill" – es handelt sich also um einen Gesetzentwurf aus dem Repräsentantenhaus des jeweiligen Staates; S.B. steht für „Senate Bill" – Gesetzentwurf des Senats des jeweiligen Staates und A.B. steht für „Assembly Bill" – Gesetzentwurf der Abgeordnetenversammlung des jeweiligen Staates.

[806] Die entsprechende LexisNexis-Recherche wurde am 06.11.2009 durchgeführt und umfasst eine Zeitspanne von 2007 bis zum Tag der Recherche.

276), Oklahoma (2009 S.B. 1164), Oregon (2007 H.B. 3277), Pennsylvania (2009 H.B. 1387), Tennessee (2007 H.B. 2190, 3412 und S.B. 2963), Virginia (2007 H.B. 2086, 2008 S.B. 1255), Washington (2007 S.B. 6020 und H.B. 1031, 2009 H.B. 1006) und Wisconsin (2009 A.B. 29).

b) Verbotsgesetzgebung

Verbotsgesetzgebung umfasst unterschiedliche Arten von Verboten. Einige Ansätze zielen darauf ab, bestimmte Verwendungen von RFID zu verbieten (meist handelt es sich um die Implantierung von RFID-Tags in Menschen). Andere verbieten das unautorisierte Auslesen von RFID-Tags zwecks Missbrauchs der enthaltenen Daten (z.B. RFID-Tags in Identifikationsdokumenten). Eine dritte Kategorie will das Tracking von Personen durch das Auslesen von RFID-Tags verbieten. Einige Transparenzansätze enthalten Regelungen zum Verbot der Kombination von RFID-Daten mit anderen Informationen über Kunden. Bemerkenswert ist, dass einige Staaten trotz der bundesgesetzlich zwingend vorgeschriebenen Einführung RFID-basierter Führerscheine (dies ergibt sich aus dem „Real ID Act“ von 2004[807]) begonnen haben, Gesetze zu erlassen, nach denen gerade die Verwendung von RFID in Führerscheinen verboten sind.[808]

Verbotsgesetzgebung fanden sich in der Vergangenheit in 17 U.S. Staaten: Alaska (2007 H.B. 65), Arkansas (2007 S.B. 195, 2009 H.B. 1978), Kalifornien (2007 S.B. 29 und 31, 2009 S.B. 544), Florida (2010 S.B. 174), Michigan (2007 H.B. 4133, 4330, 4453 und 1471, H.B. 5605, 2009 H.B. 4497 und S.B. 281), Missouri (2009 H.B. 632), Nevada (2009 S.B. 125), New Hampshire (2007 H.B. 686, 2009 H.B. 478), New York (2009 A.B. 276), North Dakota (2007 S.B. 2415), Oklahoma (2009 H.B. 1363, S.B. 1190), Oregon (2007 H.B. 3277), Rhode Island (2007 H.B. 8027, S.B. 474, 2113, 2009 H.B. 6059 und S.B. 211), Tennessee (2007 H.B. 3412 und S.B. 2963), Texas (2007 H.B. 1925, 2009 H.B. 4439, 1506 und S.B. 1902), Virginia (2008 S.B. 841, S.B. 1255), Washington (2007 H.B. 1031, 2729, 2838, 2998 und S.B. 6425, 2009 H.B. 1011) und Wisconsin (2007 A.B. 141, 2009 A.B. 29).

c) IT-Sicherheitsgesetzgebung

IT-Sicherheitsgesetzgebung verlangt bestimmte IT-Sicherheitsstandards für RFID-Anwendungen. Die Ansätze verfolgen die These, dass *privacy* besser geschützt wird, je schwieriger – und im besten Falle unmöglich – Missbrauch und unautorisiertes Auslesen sind. Solche Regelungen finden sich hauptsächlich in den Gesetzen zu den RFID-basierten Führerscheinen.[809]

---

[807] “RealID Act of 2005” (H.R. 418, 2005), später Title II des “Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005” (H.R. 1268, 2005).

[808] Vgl. hierzu oben B.II.5.b).

[809] Dies bezieht sich auf die Sicherheitsstandards für maschinenlesbare Identifikationsdokumente des U.S. Department for Homeland Security (DHS), Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, “Minimum Standards for Driver’s licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes”, S. 75, oben Fn. 168.

Einige Transparenzansätze wiederum beinhalten auch die Pflicht, Schutzhüllen aus Aluminiumfolie an die Empfänger neuer Führerscheine auszuhändigen, mit denen unautorisiertes Auslesen verhindert werden kann.[810] Weiterhin bestimmen einige Regelungen IT-Sicherheitsstandards dort, wo personenbezogene Daten beim Verkauf RFID getaggter Produkte involviert sind.[811]

IT-Sicherheitsgesetzgebung ist rechtsgeschichtlich nachweisbar in sechs U.S. Staaten: Arkansas (2007 H.B. 421 und S.B. 293), Arizona (2009 H.B. 2507 und S.B. 1143), Kalifornien (2007 S.B. 30), Michigan (2007 H.B. 5535), Minnesota (2009 H.B. 928, 1005, S.B. 345 und 1455) und Vermont (2007 H.B. 691 und S.B. 358).

d) U.S. RFID-Gesetzgebung am Beispiel New York

Der Staat New York ist seit Jahren sehr aktiv im Bereich spezialgesetzlicher RFID-Gesetzgebung. Bereits seit der Legislaturperiode 2006/2007 wurden in jeder neuen Periode Vorschläge für RFID-Gesetze mit unterschiedlichem Regelungsinhalt vorgeschlagen – jedoch bis jetzt nicht verabschiedet. Als Vorreiter sollen die in New York eingebrachten Vorschläge kurz dargestellt werden.

In der Legislaturperiode 2011/2012 sind sieben Gesetzesinitiativen zur Regelung von RFID-Sachverhalten von Mitgliedern des Senats und der Versammlung (*assembly*) – sog. Sponsoren – vorgelegt worden (A.B. 894[812], A.B. 1032[813], A.B. 1033[814], A.B. 8379[815], A.B. 8428[816], S.B. 1168[817] und S.B.1821[818]). Diese sind teilweise deckungsgleich. A.B. 894 und A.B. 8379 behandeln das *Labeling* von mit RFID getaggten Produkten, A.B. 1032 und S.B.1821 fordern die Einberufung einer RFID *Task Force* und A.B. 1033, A.B. 8428 sowie S.B. 1168 dienen als Grundlage für die Verabschiedung des „*RFID Right to Know Act*“.[819] Hinsichtlich der oben dargestellten verschiedenen RFID-Gesetzgebungsarten sind alle New Yorker Gesetzesinitiativen unter Transparenzgesetzgebung zu fassen.

---

[810] Vgl. 2009 MT S.B. 154, abrufbar unter http://data.opi.mt.gov/bills/2009/billpdf/SB0154.pdf (04.04.2013).

[811] Vgl. 2007 AK H.B. 421, abrufbar unter http://www.legis.state.ak.us/basis/get_bill_text.asp?hsid=HB0421A&session=25 (04.04.2013) und S.B. 293, abrufbar unter http://www.legis.state.ak.us/basis/get_bill_text.asp?hsid=SB0293A&session=25 (04.04.2013).

[812] http://assembly.state.ny.us/leg/?default_fld=&bn=A00894&term=2011&Summary=Y&Text=Y (04.04.2013).

[813] http://assembly.state.ny.us/leg/?default_fld=&bn=A01032&term=2011&Summary=Y&Text=Y (04.04.2013).

[814] http://assembly.state.ny.us/leg/?default_fld=&bn=A01033&term=2011&Summary=Y&Text=Y (04.04.2013).

[815] http://assembly.state.ny.us/leg/?default_fld=&bn=A08379&term=2011&Summary=Y&Text=Y (04.04.2013).

[816] http://assembly.state.ny.us/leg/?default_fld=&bn=A08428&term=2011&Summary=Y&Text=Y (04.04.2013).

[817] http://assembly.state.ny.us/leg/?default_fld=&bn=S01168&term=2011&Summary=Y&Text=Y (04.04.2013).

[818] http://assembly.state.ny.us/leg/?default_fld=%0D%0A&bn=S01821&term=2011&Summary=Y&Text=Y (04.04.2013).

[819] Eine vergleichbare Kategorisierung hat bereits vorgenommen *Schmid*, Radio Frequency Identification Law Beyond 2007 *in*: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, S. 207 ff.

Von den Initiativen aus der Legislaturperiode 2011/2012 ist keine verabschiedet worden. In der laufenden Legislaturperiode 2013/2014[820] sind bereits erneut zwei Gesetzentwürfe von unterschiedlichen Sponsoren auf den Weg gebracht worden.[821]

aa) Labeling Gesetzgebung

Die Entwürfe zur *Labeling* Gesetzgebung fordern die Kennzeichnung von mit RFID getaggten Einzelhandelsprodukten bzw. Verpackungen solcher Produkte. Enthalten sind zudem Vorschläge für die Standardisierung der zu verwendenden Kennzeichen. Weiterhin wird die Durchsetzung der Regelungen durch den Generalstaatsanwalt und die Möglichkeit einstweiliger Verfügungen und zivilrechtlicher Strafen geregelt.

Die Gesetzentwürfe beschränken sich in ihrer Definition zu RFID-Tags auf solche, die eine eindeutige Identifikationsnummer gespeichert haben. Die Pflicht zur Kennzeichnung trifft nicht nur Einzelhändler, die getaggte Produkte verkaufen sondern bereits die Hersteller solcher Produkte bzw. deren Verpackung. Das zu verwendende Kennzeichen muss die Verbraucher mindestens darüber informieren, dass das angebrachte RFID-Tag vor und nach dem Kauf eindeutige Identifikationsmerkmale übertragen kann, es muss in einer auffälligen Position angebracht sein und es muss so groß und auffällig gestaltet sein, dass es sich deutlich von dem Produkt bzw. seiner Verpackung abhebt. Für jede Zuwiderhandlung – also jeden Verkauf eines nicht ordnungsgemäß gekennzeichneten Produkts – soll der verantwortlichen Stelle eine zivile Strafe von U.S. $ 100 bis $ 1000 auferlegt werden können. Der Generalstaatsanwalt kann zusätzlich einen Antrag auf einstweilige Verfügung bei Gericht auf Anordnung der Unterlassung solcher Zuwiderhandlungen stellen.

bb) Task Force Gesetzgebung

Per Gesetz soll eine *automatic identification*-Task Force eingesetzt werden, die den Gouverneur und den Gesetzgeber neben anderen Technologien hauptsächlich über bestehende auf RFID-Szenarien anwendbare Gesetze, Programme und Verhaltensregeln informieren soll. Die Task Force soll zudem über die Datenschutzherausforderungen im Zusammenhang mit RFID informieren sowie aktuelle sowie erwartete Entwicklungen in möglichen Anwendungen von RFID beobachten sowohl die datenschutzrechtlichen Herausforderungen als auch die möglichen Vorteile für Verbraucher und Wirtschaft betreffend. Die Task Force soll mit Vertretern hoher politischer Ämter (u.a. Staatssekretär, Generalstaatsanwalt, Bürgermeister der Stadt New York) sowie elf zu bestimmenden Mitgliedern besetzt werden.

cc) Right-to-Know Gesetzgebung

Der *Right to Know Act* fordert neben der bereits im Rahmen der *Labeling* Gesetzgebung vorgesehenen Kennzeichnung von mit RFID-getaggten Einzelhandelsprodukten auch einen gene-

[820] Die Untersuchung fand am 02.04.2013 statt.

[821] „RFID Right to Know Act“, S.B. 3099, abrufbar unter http://assembly.state.ny.us/leg/?default_fld=&bn=S03099&term=2013&Summary=Y&Text=Y (04.04.2013), “RFID Task Force”, S.B. 3195, abrufbar unter http://assembly.state.ny.us/leg/?default_fld=&bn=S03195&term=2013&Summary=Y&Text=Y (04.04.2013).

rellen Hinweis über die Verwendung von RFID in den Geschäftsräumen des Einzelhändlers. Entsprechende Hinweisschilder sollen entweder an jeder Kasse oder aber so angebracht sein, dass sie von jeder Kasse aus gut sichtbar sind. Neben dem Hinweis auf die Verwendung von RFID sollen die Kunden auch auf die Pflicht des Einzelhändlers zur Entfernung oder Deaktivierung der RFID-Tags vor dem Verlassen der Geschäftsräume hingewiesen werden. Die Kosten für Deaktivierung oder Entfernung sind vom Einzelhändler zu tragen. Gleichfalls sollen die Kunden auf ihr Recht hingewiesen werden, bei dem Einzelhändler die Herausgabe aller über sie mittels RFID gespeicherten persönlichen Informationen zu beantragen. Entsprechende Antragsformulare hat der Einzelhändler bereit zu halten. Das Gesetz würde es Einzelhändlern auch verbieten, ihre Kunden mittels faktischen Zwangs dazu zu bewegen, auf eine Deaktivierung oder Entfernung der RFID-Tags zu verzichten, indem für Rückgabe- und Gewährleistungsrechte das Vorhandensein eines aktivierten RFID-Tags vorausgesetzt wird. Eine Reaktivierung bereits deaktivierter Tags würde von der ausdrücklichen Zustimmung des Kunden abhängig gemacht. Die Kombination von RFID-Daten mit sonstigen persönlichen Daten der Kunden würde ebenso verboten wie die Weitergabe der mittels RFID gewonnenen Daten zwecks Identifikation der Kunden. Die Durchsetzung des Gesetzes obläge mittels Beantragung einstweiliger Verfügungen wie bei der *Labeling* Gesetzgebung dem Generalstaatsanwalt. Für jede Zuwiderhandlung soll das Gericht eine Strafe von bis zu U.S. $ 500 anordnen können.

F. Bewertung und Fazit

I. Neue Herausforderungen aufgrund technologischer Besonderheiten

Im Verhältnis zu anderen Auto-ID-Technologien wie dem Barcode zeichnet sich RFID dadurch aus, dass die auf den Tags gespeicherten Daten über bestimmte physikalisch bedingte Distanzen ausgelesen werden können, ohne dass hierfür ein optischer oder sonstiger physischer Kontakt zwischen Tag und Lesegerät erforderlich ist. Diese technologischen Begebenheiten machen RFID zu einem großen Hoffnungsträger der Wirtschaft; insbesondere sein Einsatzpotenzial auf Produktebene – durch Ersetzung des Barcodes – kündigt eine flächendeckende Verbreitung und damit den ubiquitären Einsatz an.

Durch teils „unsichtbare“ weil in das Produkt bzw. dessen Verpackung eingearbeitete Tags sowie in Umgebungsgegenstände eingebaute Lesegeräte ergibt sich ein Potenzial unüberschaubarer Auslesevorgänge sowohl Qualität als auch Quantität betreffend: Mangels Erkennbarkeit verbleibt dem Betroffenen ohne entsprechende technische Hilfsmittel keine Kontrollmöglichkeit weder hinsichtlich autorisierter noch unerlaubter Auslesevorgänge.

Hierdurch kann sich ein Gefühl allgegenwärtiger Überwachung bei den Betroffenen einstellen, besteht doch die Gefahr, dass der Leitsatz des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht in einer ubiquitären RFID-Umgebung unterminiert wird: Der Betroffene weiß dann eben gerade nicht mehr, wer was wann und bei welcher Gelegenheit über ihn weiß. Diese zurzeit sicher noch diffuse Angst droht sich ohne entsprechende Gegenmaßnahmen zu realisieren. Bei Ergreifen von Gegenmaßnahmen ist aber zu berücksichtigen, dass die Technologie bis jetzt nicht wie noch vor wenigen Jahren angenommen flächendeckend verwendet wird, zurzeit noch nicht von einer ubiquitären RFID-Infrastruktur gesprochen werden kann. Es muss also ein Ausgleich zwischen dem drohenden Risikopotenzial und den tatsächlichen Gegebenheiten geschaffen werden, der heute und perspektivisch auch in der Zukunft den Datenschutzinteressen der Betroffenen auf der einen und den wirtschaftlichen Interessen der RFID verwendenden Unternehmen auf der anderen Seite gerecht wird.

II. Traditionelles Datenschutzrecht

Im Bereich des traditionellen Datenschutzrechts ist zunächst zu berücksichtigen, dass für einzelne RFID-Anwendungen bereits spezielle Regelungen bestehen. Hier sind besonders die Vorschriften im Pass- und Ausweisrecht hervorzuheben. Sie regeln nicht nur besondere technische Voraussetzungen, die RFID in diesen Bereichen erfüllen muss, sondern auch die Berechtigungen zur Datenauslesung und -verarbeitung und zwar sowohl für öffentliche als auch für nicht-öffentliche Stellen. Sonstige RFID-Anwendungen sind heute nach den allgemeinen Regelungen und hier maßgeblich dem BDSG zu beurteilen.

Das BDSG ist ausgelegt auf einzelne Datenverarbeitungsvorgänge – nicht auf allgegenwärtige massenhafte Datenverarbeitungen, wie sie in RFID-Anwendungen zu erwarten sind. Daher rührt auch das bisherige Verständnis des Begriffs der personenbezogenen Daten. Dieser ist zu eng bzw. zu starr für die Herausforderungen des mit RFID informatisierten Alltags. Nach bis-

herigem Verständnis und verbreiteter Auffassung würde ein Großteil aller RFID-Anwendungen – nämlich alle, in denen auf den RFID-Tags lediglich eine Identifikationsnummer gespeichert ist – nicht in den Anwendungsbereich des traditionellen Datenschutzrechts fallen. Dies ist ein unhaltbarer Zustand. Die aufgezeigten Szenarien machen deutlich, dass Gefahren für das informationelle Selbstbestimmungsrecht des Einzelnen – nämlich in Form von Tracking und Profilbildung – auch bei diesen Anwendungen besteht.

Die Einführung des Begriffs der personen*beziehbaren* Daten hilft hier nicht weiter. Der Begriff der personenbeziehbaren Daten ist nach diesseitiger Auffassung ohnehin bereits im traditionellen Konzept verankert und müsste von daher nicht neu im Gesetz geregelt werden. Er trägt zudem nicht zur Lösung der bestehenden Probleme bei: Selbst wenn man die EPC-Identifikationsnummern unter diesen Begriff fassen würde, stellten sich im weiteren Probleme bei der Anwendung der bestehenden datenschutzrechtlichen Regeln.

Darüber hinaus wird teilweise kritisiert, es mache wenig Sinn alle Formen der Datenverarbeitung in einer informatisierten Welt des *ubiquitous computing* einheitlichen Anforderungen zu unterwerfen.[822] Es wird vorgeschlagen, zwischen Datenverarbeitungen mit gezieltem und solchen ohne gezielten Personenbezug zu unterscheiden und beide unter verschiedene Regelungssysteme zu stellen.[823] Verarbeitungen mit gezieltem Personenbezug sollten solche sein, deren Zweck eine personenbezogene oder personenbeziehbare Verwendung ist. Verarbeitungen ohne einen solchen gezielten Personenbezug sollten gerade nicht den Zweck der personenbezogenen oder personenbeziehbaren Verwendung verfolgen. Für Datenverarbeitungen mit gezieltem Personenbezug solle auf die traditionellen datenschutzrechtlichen Regelungen zurückgegriffen werden. Für solche ohne gezielten Personenbezug sollten die Anforderungen „risikoadäquat und effizienzsteigernd spezifiziert“ werden.[824] Die Ansicht geht indes davon aus, dass es bei bestimmten Datenerhebungen (und Verarbeitungen) an einem überhaupt zielgerichteten Verhalten fehlt, die Daten also quasi mit anfallen ohne gewollt zu sein. Dies wäre in RFID-Anwendungen immer dann denkbar, wenn die verantwortliche Stelle – z.B. ein Supermarktbetreiber – lediglich die von ihr ausgegebenen Tags gezielt einlesen möchte – z.B. um Geschäftsabläufe zu optimieren – und dabei alle anderen von einer Person bereits in die Geschäftsräume mitgebrachten RFID-Tags – z.B. in der Kleidung – wegen technischer Kompatibilität ungezielt mit einliest. Bei der Verarbeitung dieser Daten sollte nach benannter Ansicht die verantwortliche Stelle verpflichtet werden, diese auf ein Minimum zu beschränken, sie einer strengen Zweckbindung zu unterwerfen und gegen Zweckentfremdung zu schützen und sie sofort nach der Verarbeitung zu löschen; jede Zweckänderung solle einem Verwertungsverbot unterworfen werden.[825]

Dieser Ansatz muss sich fragen lassen, ob er noch mit den Vorgaben des Bundesverfassungsgerichts zu vereinbaren ist. Zwar geht dieses selbst davon aus, dass es bei der Feststellung der

[822] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 68.

[823] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 69.

[824] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 69.

[825] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, oben Fn. 334, S. 69.

persönlichkeitsrechtlichen Bedeutung eines Datums – und wohl auch der konkreten Verarbeitung – immer auf den spezifischen Verwendungszusammenhang ankommt, mithin nicht alle Datenverarbeitungen das gleiche Gefährdungspotenzial aufweisen.[826] Es betont aber auch, dass es unter den Bedingungen der automatischen Datenverarbeitung – also erst recht in einer informatisierten Welt des *ubiquitous computing* – kein „belangloses Datum" mehr gibt.[827] Entscheidend soll von daher gerade nicht nur der konkrete Verwendungszweck sondern die Verwendungs*möglichkeit* sein.[828] Hier dürfte der springende Punkt liegen: Die bloße Möglichkeit weitergehender Verwendung – und genau das wird hinsichtlich unbemerkt angefertigter Profile befürchtet – führt bereits zu einem entsprechend hohen Gefahrpotenzial für das informationelle Selbstbestimmungsrecht des Einzelnen. Das Schicksal weniger „gefahrträchtiger" Daten alleine in die Hände der verantwortlichen Stelle zu legen – so wie von der aufgezeigten Ansicht proklamiert – dürfte von daher nicht den vom Bundesverfassungsgericht aufgestellten Anforderungen genügen. Vielmehr wird es auch hier verstärkt auf Transparenz und Information ankommen, die es dem Einzelnen ermöglichen, selbst Kontrolle über seine Daten auszuüben.

Die Konstruktion des traditionellen Datenschutzrechts mit dem Grundsatz präventiven Verbots mit Erlaubnisvorbehalt ist grundsätzlich der richtige Ansatz um dem Betroffenen eine möglichst umfassende Kontrolle über seine eigenen Daten zu geben. Solange aber neben der Rechtfertigung mittels Einwilligung auch noch die Rechtfertigungstatbestände der §§ 28 ff. BDSG bestehen, wird dieser Schutzzweck untergraben. Die unbestimmten Rechtsbegriffe und die technikneutrale Ausgestaltung lassen den datenverarbeitenden Stellen zu viele Freiräume, in denen der Betroffene trotz der bestehenden Informationspflichten wiederum seiner Kontrollmöglichkeit beraubt wird.

Die traditionelle Einwilligung indes ist in einer Welt der ubiquitären Datenverarbeitung mittels RFID nicht praktikabel. Für jeden einzelnen Datenverarbeitungsvorgang eine spezifische, den formellen Anforderungen genügende Einwilligungserklärung vom Betroffenen einzuholen ist schlechterdings unmöglich. Damit wird das Konzept konterkariert und behindert mehr, als dass es zu einem umfassenden Schutz beitrüge. Die Konsequenz könnte nur sein, das Einwilligungserfordernis abzuschaffen oder aber es so anzupassen, dass pauschale Einwilligungserklärungen vorab möglich wären. Dies könnte insbesondere durch die Verwendung einer „P3P" ähnlichen Struktur mittels RFID-Protokollen erreicht werden. Der Betroffene könnte durch einen mitgeführten elektronischen Berechtigungskatalog vorab festlegen, wer, wann, wie und in welchem Umfang auf die von ihm mitgeführten RFID-Tags zugreifen darf. Voraussetzung wäre natürlich, dass die hierfür erforderliche Infrastruktur flächendeckend verwendet wird und sich alle verantwortlichen Stellen an die Vorgaben des Betroffenen halten. Dies könnte gegebenenfalls gesetzlich vorgegeben werden.

[826] BVerfGE, 65, 1 (45) – Volkszählung.

[827] BVerfGE 65, 1 (45) – Volkszählung.

[828] BVerfGE 65, 1 (45) – Volkszählung.

Auch der künftige Umgang mit den sonstigen Konzepten des traditionellen Datenschutzrechts– maßgeblich Direkterhebungsgrundsatz, Grundsatz der Datenvermeidung und Datensparsamkeit – wird davon abhängen, wie EPC und vergleichbare Identifikationsnummern eingeordnet werden. Die Durchsetzung dieser Konzepte wird in einer ubiquitären RFID-Umgebung scheitern, stehen sie doch massenhafter Datensammlung diametral entgegen. Qualifizierte man produktbezogene Identifikationsnummern als personenbezogene Daten und unterwürfe sie damit dem Regime des traditionellen Datenschutzrechts müssten die Grundsätze fundamental überdacht und an die Gegebenheiten der informatisierten Welt angepasst werden. Eine Übertragung der Grundsätze auf spezielle RFID-Gesetze machte folglich keinen Sinn.

III. Ansätze einer RFID-spezifischen Gesetzgebung

Die bis heute vorgebrachten Vorschläge für eine spezielle RFID-Datenschutzgesetzgebung – die Sonderregelungen des Pass- und Ausweisrechts einmal ausgenommen – beziehen sich vornehmlich auf den privatwirtschaftlichen Bereich und damit hauptsächlich auf die vorgestellten EPC-Szenarien.

Die von der EU-Kommission verabschiedete Empfehlung zu RFID ist der erste gesetzgeberische Akt zu RFID auf EU-Ebene. Sie beinhaltet vier Regelungskonzepte: Datenschutzfolgenabschätzung, Information und Transparenz, Spezifika für den Einsatz im Einzelhandel sowie *Privacy-by-Design*.

Die Vorgabe an die Wirtschaft vor Einführung von RFID-Anwendungen Datenschutzfolgenabschätzungen durchzuführen ist eine (erste) Maßnahme im Bereich der (regulierten) Selbstregulierung. Sie dient vornehmlich der Risikoanalyse und selbstverantwortlichen Prüfung, ob die geplante Anwendung mit dem geltenden – also dem traditionellen – Datenschutzrecht vereinbar ist. Die Schaffung von weitergehenden Pflichten im Wege einer Selbstregulierung verlangt die Kommission nicht von den Betreibern. Die Schaffung solcher Selbstverpflichtung ist aber bereits im europäischen und auch deutschen Datenschutzrecht angelegt.

Die weiterhin in der Empfehlung geforderten Transparenz- und Informationspflichten für RFID-Anwendungsbetreiber stellen im Wesentlichen Klarstellungen zu den bereits bestehenden Informationspflichten dar. Wo personenbezogene Daten verarbeitet werden, ergeben sich diese bereits aus dem traditionellen Datenschutzrecht. Aber auch wo keine personenbezogenen Daten verarbeitet werden, sollen die Hinweispflichten gelten (dies ergibt sich im Umkehrschluss aus Punkt 7 c der Empfehlung). Erweiterungen ergeben sich maßgeblich bzgl. der Ergebnisse der Datenschutzfolgenabschätzung (Punkt 7 d) der Empfehlung) sowie der Pflicht vorhandene Lesegeräte kenntlich zu machen (Punkt 8 der Empfehlung).

Besonders für den Einzelhandel soll weiterhin auch eine Kennzeichnungspflicht für jedes einzelne auf einem Produkt angebrachte RFID-Tag gelten. Außerdem sollen diese grundsätzlich noch innerhalb der Geschäftsräume deaktiviert bzw. entfernt werden, ohne dass den Kunden hieraus Nachteile im Hinblick auf ihre Rechte (Gewährleistungsrechte u.ä.) entstehen dürfen.

Die Berücksichtigung des *Privacy-by-Design*-Ansatzes in RFID-Anwendungen bildet eine fortwährende Entwicklung auf europäischer Ebene ab. Datenschutz wird zunehmend von der technischen Ausgestaltung von Systemen und einzelnen Systemkomponenten abhängen.

Auf deutscher Ebene gibt es bis jetzt keinen Gesetzesvorschlag zur Regelung von RFID-Anwendungen. Die Entschließung des Bundesrats zur Umsetzung der Empfehlung ist die jüngste Maßnahme auf dem Weg zur Vorbereitung eines solchen Gesetzentwurfs. Über den Regelungsgehalt der Empfehlung hinausgehende Forderungen wurden vom Bundesrat überdies nicht gestellt. Es wird aber deutlich, dass eine verstärkte Tendenz zur Forderung selbstverantwortlichen Handelns der Wirtschaft mittels speziell entwickelter Selbstverpflichtungen besteht.

Das Beispiel spezifischer RFID-Gesetzgebung aus dem U.S. Staat New York war lange Jahre revolutionär, bleibt jedoch nunmehr hinter den Vorgaben der EU-Empfehlung zurück. Der New Yorker Gesetzgeber setzt – so wie viele andere – vornehmlich auf Kontrolle und Selbstbestimmung durch Transparenz und Information der Betroffenen. Hierzu gehören nicht nur Hinweisschilder und Kennzeichen auf getaggten Produkten und Lesegeräten sondern auch die grundsätzliche Pflicht zur Deaktivierung der Tags an der Kasse sowie das Verbot, die Kunden faktisch zu zwingen, auf die Deaktivierung zu verzichten, indem Gewährleistungsrechte u.ä. von der Existenz eines funktionsfähigen RFID-Tags abhängig gemacht werden.

Die vorgeschlagenen Regelungen setzen sich allseits nicht mit der essenziellen Frage des Begriffs der personenbezogenen Daten auseinander, was erforderlich wäre, um eine Klärung der Frage herbeizuführen, welche Regelungen des traditionellen Datenschutzrechts bereits jetzt auf RFID-Anwendungen anwendbar sind und in welchen Bereichen gegebenenfalls weitergehender gesetzgeberischer Bedarf besteht. Die Vorschläge verlegen sich vielmehr alle auf Ergänzungen des bestehenden Rechtsrahmens, maßgeblich durch Erweiterung der Transparenz- und Informationspflichten. Bemerkenswert ist, dass in Einzelhandelsanwendungen allseits eine Deaktivierung der verwendeten RFID-Tags gefordert wird. Dies verdeutlicht, dass die bestehenden Gefahrpotenziale auch von den Gesetzgebern anerkannt werden. Abgesehen von Tracking und Profilbildung innerhalb der Geschäftsräume der verantwortlichen Stelle würden bei Durchsetzung einer solchen Deaktivierungspflicht weitergehende Gefahren ausgeschlossen. Dies stellt auf den ersten Blick einen Schritt in die richtige Richtung dar. Außen vor bliebe bei einem solchen Vorgehen allerdings, dass zum einen die *In-House*-Problematik nicht gelöst würde und zum anderen weitergehende Vorteile von RFID – maßgeblich für den Betroffenen aber auch nachgelagerte Wirtschaftszweige wie Hersteller von Haushaltselektronik – abgeschnitten würden. Die standardmäßige Deaktivierung bzw. Entfernung der RFID-Tags auf Einzelhandelsprodukten kann damit nur dann einen sinnvollen und akzeptablen Beitrag zur Lösung der bestehenden Herausforderungen liefern, sofern, wie von der EU-Empfehlung vorgeschlagen, dem Betroffenen die Möglichkeit verbleibt, auf die Deaktivierung bzw. Entfernung durch Erteilung seiner Einwilligung zu verzichten.

Wichtig ist die Erweiterung bzw. Verdeutlichung der Transparenz- und Informationspflichten auch unter Einbeziehung von Kennzeichen auf getaggten Produkten und Lesegeräten. Nur ein informierter Betroffener kann von weitergehenden Rechten Gebrauch machen oder sich aber

gänzlich der betreffenden Anwendung entziehen – dies gilt indes nur, solange noch keine flächendeckende Verwendung von RFID gegeben ist.

In die richtige Richtung gehen auch die insbesondere auf deutscher Ebene laut gewordenen Forderungen nach mehr Selbstverantwortung der Wirtschaft durch sektor- bzw. anwendungsspezifische Selbstverpflichtungen. Allerdings kann und darf der Wirtschaft nicht etwas aufgebürdet werden, zu dem originär der Gesetzgeber verpflichtet ist: Der Schutz des informationellen Selbstbestimmungsrechts ist durch Schaffung entsprechender gesetzlicher Regelungen eben diesem vom Bundesverfassungsgericht auferlegt worden. Möglich und sinnvoll ist eine Verstrebung der Instrumente der Gesetzgebung und der Selbstregulierung im Wege einer regulierten Selbstregulierung. Sofern der Gesetzgeber die Rahmenvorgaben zum Schutz personenbezogener Daten macht, kann die Wirtschaft passgenaue und flexible Anwendungskonzepte erstellen, die diesen Rahmen ausfüllen. Die Erstellung einer Datenschutzfolgenabschätzung, wie von der Kommission gefordert, ist hierbei ein guter erster Schritt. Indes wäre zu eruieren, ob nicht weitergehende Pflichten zur Erstellung von durchsetzbaren Selbstverpflichtungserklärungen – etwa in Anpassung der bereits vorhandenen Regelungen in Artikel 27 DSRL sowie § 38a BDSG – einer rein freiwilligen Lösung vorzugswürdig sind.

Neben Selbstverpflichtungen der Wirtschaft sieht das traditionelle Datenschutzrecht bereits die Durchführung von Datenschutzaudits mit anschließender Zertifizierung vor. Hier besteht indes Ausbaubedarf: Mangels klarer Vorgaben, wie Datenschutzaudits abzulaufen haben und wann Datenschutzzertifikate verliehen werden können bzw. sollen, hat sich kein einheitliches System herausgebildet. Erkannt hat der Gesetzgeber dies, sieht er doch die Schaffung eines Datenschutzauditgesetzes bereits in § 9a Satz 2 BDSG ausdrücklich vor. Diese selbstgeschaffene Vorgabe muss er alsbald erfüllen, damit Selbstregulierungsmaßnahmen der Wirtschaft von unabhängigen Stellen nach allgemein anerkannten Standards überprüfbar und die Bemühungen von Unternehmen per Gütesiegel wettbewerbswirksam werden.

IV. Regelungsbedarf

Der vom europäischen und deutschen Gesetzgeber bis jetzt verfolgte Ansatz der Technikneutralität ist grundsätzlich begrüßenswert. Lange hat er auch vollkommen ausgereicht, um datenschutzrechtlichen Herausforderungen zu begegnen. Mit zunehmender Technisierung und Informatisierung stößt er allerdings an Grenzen. Dies rührt wie festgestellt zu wesentlichen Teilen daher, dass der Begriff der personenbezogenen Daten wie in der DSRL und dem BDSG vorausgesetzt kaum mehr geeignet ist, alle Daten mit regelungsbedürftigem Gefahrpotenzial eindeutig zu kategorisieren. Dies zeigt sich am Beispiel RFID besonders deutlich.[829] Mit den oben dargestellten Ausführungen könnte man diese Unklarheiten ausräumen: Unter Zugrundelegung des oben angewendeten Leitfadens wären grundsätzlich alle Daten auf RFID-Tags personenbezogene, sofern sie von Personen mitgeführt werden, unabhängig davon, ob es sich um soziale Identifikatoren – also personenbezogenen Daten im konventionellen Sinne – oder um (produktbezogene) Identifikationsnummern handelt. Die Nachteile einer solchen Sicht-

[829] Ähnliches gilt für IP-Adressen, vgl. hierzu oben D.III.

weise sind offensichtlich: Alle möglicherweise nur rein hypothetisch risikobehafteten Daten dem Regime des Datenschutzrechts zu unterwerfen, führte zu gravierenden wirtschaftlichen Einschnitten. Die Wirtschaft sähe sich enormen Herausforderungen gegenüber, sofern sie weiterhin RFID auch im Endkundenbereich einsetzen wollte. Zum einen wäre der komplette Verzicht auf eindeutige Identifikationsnummern oder Lesegeräte jedenfalls ab dem Moment, in dem getaggte Produkte in den Endkundenbereich gelangen denkbar – womit sich die Frage des Mehrwerts von RFID gegenüber anderen Auto-ID-Systemen stellte. Weiterhin käme der Einsatz von *Privacy Enhancing Technologies* in Betracht, um die Anonymität der Endkunden sicherzustellen.

Solange RFID nicht in einem Mindestumfang im Endkundenbereich Verwendung findet, stellen sich diese Konsequenzen indes als überzogen dar. Von schweren Eingriffen in das informationelle Selbstbestimmungsrecht oder auch nur erheblichen Gefahren für es kann zum jetzigen Zeitpunkt (produktbezogene) Identifikationsnummern betreffend nicht gesprochen werden. Vor diesem Hintergrund stellt sich zunächst eine Notwendigkeit dar: Es muss klar sein, welche RFID-Daten unter das Regime des jetzt geltenden Datenschutzrechts fallen sollen und welche nicht. Dies ist zwingend erforderlich, um der Wirtschaft den nötigen Handlungsfreiraum für die Entwicklung neuer Geschäftsmodelle zu geben. Hierfür muss der Begriff der personenbezogenen Daten überarbeitet und an die neuen Gegebenheiten angepasst werden.[830] Es muss deutlich herausgearbeitet werden, wie das Bestimmtheitselement der Definition auszulegen ist, wann also Daten mit oben vorgestelltem Begriff noch „personen*beziehbar*“ sind und wann es sich um faktisch anonyme Daten handelt.

In einem weiteren Schritt stellt sich die Frage, wie – sollte man sich entschließen (produktbezogene) Identifikationsnummern nicht als personenbezogene Daten zu qualifizieren – mit der Problematik des Tracking und der Profilbildung umgegangen werden soll. Dies gilt zum einen innerhalb der RFID-Umgebung, in der die betreffenden RFID-Tags ausgegeben werden – also den Geschäftsräumen der primär verantwortlichen Stelle – als auch außerhalb, sprich im öffentlichen Raum bzw. RFID-Umgebungen Dritter. Tracking und Profilbildung im Außenbereich ließen sich wirksam mit der verbreitet vorgeschlagenen Pflicht zur Deaktivierung bzw. Entfernung der Tags noch in den Räumen der Tag ausgebenden Stelle – also spätestens an der Kasse – erreichen. Tracking und Profilbildung bereits innerhalb der RFID-Umgebung der Tag ausgebenden Stelle ließen sich zum einen verhindern, indem die Tags bereits vor Bereitstellung im Endkundenbereich deaktiviert bzw. entfernt würden. Zum anderen könnten *Privacy Enhancing Technologies* verwendet werden. Denkbar wäre hier maßgeblich die Aushändigung von Blocker-Tags an die Kunden bei Betreten der Geschäftsräume. Jedenfalls im Einzelhandel dürften Verschlüsselungsmechanismen wegen der vorausgesetzten Komplexität und damit Kosten der zu verwendenden RFID-Tags ausgeschlossen sein. Eine entsprechende Standardisierung vorausgesetzt könnten wohl die ebenfalls angesprochenen RFID-Protokolle i.S. einer *Platform for Privacy Preferences* (P3P) zum Einsatz kommen. Ein generelles Ver-

[830] Ähnlich unter Verweis auf die neuen Gegebenheiten der „digitalen Welt“ die Vertreter der Oppositionsfraktionen in der Enquête-Kommission, vgl. Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 113.

bot von Tracking und Profilbildung erscheint indes zum jetzigen Zeitpunkt überzogen. Das wirtschaftliche Interesse an der Verwendung der RFID-Technologie zur Analyse ist zu berücksichtigen. Solange kein missbräuchliches Verhalten zu Lasten der Betroffenen droht, erscheinen sensible Lösungen basierend auf Information, Zusammenwirken und Vertrauen vorzugswürdig. Sinnvoll erscheint es allerdings, die Wirtschaft in den Bereichen, in denen keine Identifizierbarkeit vorausgesetzt ist, zu verpflichten „anonyme" Daten für ihre Zwecke einzusetzen. Gemeint sind hierbei nicht anonyme Daten i.S.d. BDSG – diese bezögen sich auf Daten, die nicht einer natürlichen Person zugeordnet werden können und aus diesem Grund nicht als personenbezogene Daten i.S.d. traditionellen Datenschutzrechts zu qualifizieren sind. Produktbezogene Identifikationsnummern sind nach weit verbreiteter Ansicht eben solche Daten. Vielmehr ist gemeint, dass diese produktbezogenen Identifikationsnummern wie der EPC so verkürzt werden, dass wann immer möglich, nicht mehr das einzelne Produkt und damit auch nicht sein Besitzer ermittelbar ist.

Als wesentlicher Bauteil eines datenschutzfreundlichen Einsatzes von RFID spielt wie in allen datenschutzrelevanten Bereichen Transparenz eine entscheidende Rolle. Wesentliches Merkmal des informationellen Selbstbestimmungsrechts ist schließlich, dass der Betroffene weiß oder jedenfalls wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß.[831] Sofern die Verarbeitung von RFID-Daten nicht bereits nach traditionellem Datenschutzrecht dem Betroffenen kenntlich gemacht werden muss, müssen solche Informationspflichten, wie es auch die EU-Empfehlung fordert und wie es der New Yorker Gesetzgeber vorsieht, neu geschaffen werden. Hierzu gehört auch die Kennzeichnung von RFID-Tags und Lesegeräten, die dem Betroffenen sonst meist verborgen bleiben würden.

Umgesetzt werden kann dies einerseits durch gesetzgeberische Maßnahmen, andererseits durch Maßnahmen der Selbstregulierung. Zwar wird die Verfolgung des Ansatzes der „regulierten Selbstregulierung" als „verwobenes Miteinander von staatlicher Regulierung einerseits und Selbstregulierung der Wirtschaft andererseits" vor dem Hintergrund des voll umfänglichen Geltungsanspruchs staatlicher Regulierung im Bereich des Datenschutzes teilweise kritisch gesehen.[832] Vorzugswürdig vor rein gesetzgeberischen Maßnahmen erscheint indes dennoch ein kombinierter Ansatz.[833] Langfristig funktionierende Selbstregulierung setzt einen gesetzlichen Rahmen voraus, der das Mindestmaß der zu regelnden Tatbestände und Vorgaben zu Abläufen und Formalien klarstellt. Die zögerliche Annahme der Möglichkeit der Erstellung von Verhaltensregeln wie in § 38a BDSG vorgesehen macht deutlich, dass es solcher Vorgaben braucht, um der Wirtschaft die nötigen Anreize für ein Tätigwerden zu bieten.[834] Zu

[831] BVerfGE 65, 1 (43) – Volkszählung.

[832] Vgl. Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft" zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 76.

[833] Für ein solches Vorgehen sprechen sich jedenfalls die Vertreter der Oppositionsfraktionen in der Enquête-Kommission aus, vgl. Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft" zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 113.

[834] So sehen dies auch die Vertreter der Oppositionsfraktionen in der Enquête-Kommission „Internet und Digitale Gesellschaft" im Zwischenbericht der Kommission zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 113.

diesem Zwecke böte sich an, sektorspezifische Ausführungsgesetze bzw. normkonkretisierende Vorschriften zu § 38a BDSG zu erlassen. In einem entsprechenden Gesetz könnten dann auch die Vorgaben der EU Empfehlung umgesetzt werden, wie vom Bundesrat gefordert.

Sollte die Wirtschaft ihrem Auftrag zur Selbstregulierung dann in einem festgelegten Zeitraum nicht oder nicht voll nachkommen, wäre der Gesetzgeber in der Pflicht, die erforderlichen Regelungen selbst vorzugeben. Um der fehlenden Flexibilität gesetzgeberischer Maßnahmen zu entgehen, ist aber zunächst im Wege einer entsprechend engen Zusammenarbeit von Wirtschaft und Politik die Erstellung von Selbstverpflichtungen anzustreben.

Als weiteren Anreiz für die Wirtschaft ist ebenfalls das Datenschutzaudit wie von § 9a BDSG vorgesehen weiter auszubauen: Das längst überfällige Datenschutzauditgesetz muss klare Vorgaben für die Auditierung sowie Zertifizierung aufstellen, damit Selbstregulierung belohnt wird und damit entsprechende Anreize für Unternehmen geschaffen werden, Datenschutz künftig stärker voranzutreiben.

Wie Datenschutz in RFID-Anwendungen am besten erreicht werden kann, wird sich sektorspezifisch unterscheiden. Ob Verhaltensregeln und/oder *Privacy-by-Design*-Merkmale in einer speziellen Anwendung zielführend und gleichzeitig wirtschaftlich sind, sollte zunächst der Wirtschaft überlassen bleiben. Auch hier gilt, dass der Gesetzgeber bei unzureichendem Tätigwerden der Wirtschaft selbst Regelungen erlassen muss.[835]

Die Entwicklungen im Bereich RFID sind fortlaufend genau zu beobachten. Nach dem Vorbild der New Yorker Gesetzgebung zur Errichtung einer *Task Force*, muss auch in Europa und Deutschland verfahren werden.[836] Die Beobachtung und Berichterstattung kann hierzulande von den bereits vorhandenen Datenschutzaufsichtsbehörden, sprich den Datenschutzbeauftragten der Länder und des Bundes, übernommen werden.

[835] Momentan ebenfalls keinen Bedarf für konkrete Vorgaben sehen offenbar auch die Vertreter der Oppositionsfraktionen in der Enquête-Kommission aus, vgl. Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 121.

[836] So auch die Vertreter der Oppositionsfraktionen in der Enquête-Kommission aus, vgl. Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, oben Fn. 334, S. 121; zwingende Vorgaben könnten indes bald aus Brüssel kommen, jedenfalls hat die Kommission bereits zum Ausdruck gebracht, dass „zur Sicherstellung der Einhaltung geeigneter Normen Maßnahmen erforderlich sind, die über eine Selbstregulierung oder den guten Willen der Akteure hinausgehen. Die Kommission wird anhand entsprechender Folgenabschätzungen prüfen, inwieweit es notwendig ist, Normen für die Verarbeitung personenbezogener Daten durch Technologien zum Schutz der Privatsphäre zu entwickeln“, Mitteilung der Kommission KOM(2007) 228 endgültig, oben Fn. 660, S. 8.

G. Ausblick

Der europäische Rechtsrahmen für den Datenschutz wird zurzeit überarbeitet. Für den Bereich RFID hat die Kommission in Punkt 20 der Empfehlung folgendes festgelegt:

> 20. Innerhalb von drei Jahren nach der Veröffentlichung dieser Empfehlung im Amtsblatt der Europäischen Union wird die Kommission einen Bericht über die Umsetzung dieser Empfehlung, ihre Wirksamkeit und ihre Auswirkungen auf die Wirtschaftsteilnehmer und Verbraucher, insbesondere über die in Nummern 9 bis 12 empfohlenen Maßnahmen, vorlegen.

Die Evaluierungsphase würde damit spätestens im Mai 2012 enden. Die Artikel-29-Datenschutzgruppe hat in ihrem Arbeitspapier zur Befürwortung des Rahmens der Branche für Datenschutzfolgenabschätzungen für RFID-Anwendungen darauf hingewiesen, dass die Umsetzung der Empfehlung in der Wirtschaft wesentlich auf der Durchführung der Datenschutzfolgenabschätzung beruht. Da der hierfür vorgelegte Rahmen allerdings erst Mitte 2011 angenommen worden ist, sei es sinnvoll, die Berichtsfrist entsprechend nach hinten zu verschieben, um eine volle Umsetzung der Regelungen der Empfehlung abzuwarten.[837] Mit der Auswertung der bis frühestens Mai 2012 gewonnenen Erkenntnisse dürfen Ergebnisse erwartet werden, anhand derer sich das Bedürfnis für gesetzgeberische und sonstige Aktivitäten zum Schutze des informationellen Selbstbestimmungsrechts wird messen lassen müssen. Folgende grundsätzliche Handlungsempfehlungen an den Gesetzgeber, die Branche und die Endnutzer sollen aber bereits jetzt ausgesprochen werden. Grundlegende Neuausrichtungen zur Begegnung der durch RFID ausgelösten Herausforderungen sind in jedem Fall erforderlich. Die Zukunft wird indes zeigen, wie Detailfragen zu klären sein könnten.

I. Handlungsempfehlung an den Gesetzgeber

Ein Aufschieben gesetzgeberischer Maßnahmen hindert die Entwicklung der RFID-Technik eher, als dass es sie fördert.[838] Die Bundesregierung unterliegt ebenso wie der Europäische Gesetzgeber einem Irrtum, wenn sie annehmen, eine datenschutzrechtliche Regulierung von RFID zum jetzigen Zeitpunkt sei verfrüht, weil die Technik nicht verbreitet sei und deshalb auch kaum bis keine Gefahren für das informationelle Selbstbestimmungsrecht des Einzelnen bestünden. Zwar ist richtig, dass sich die einstigen Prognosen eines flächendeckenden RFID-Einsatzes bis heute nicht bestätigt haben. Nichts desto trotz gibt es heute bereits in zahlreichen verbraucher- und endkundensensiblen Bereichen RFID-Anwendungen, die Datenschutzrisiken begründen. Alleine aus diesem Grund, ist der Gesetzgeber aufgerufen, klare Vorgaben für den Einsatz von RFID zu schaffen. Gerade das Fehlen solch klarer Vorgaben dürfte – neben rein wirtschaftlichen Erwägungen – zudem auch einer der tragenden Gründe sein, warum die RFID-Technik es bis heute nicht geschafft hat, ihr Potenzial in den oben benannten Anwendungsbereichen zu realisieren. Die Unsicherheiten in der Branche sind nicht zu unter-

[837] Artikel-29-Datenschutzgruppe, WP 180, oben Fn. 339, S. 6.

[838] Vgl. BITKOM Pressemittelung vom 06.04.2011, Selbstverpflichtung zum Datenschutz bei RFID, oben Fn. 726; ebenso Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S.100.

schätzen. Statt mit ihrer „*laisser faire*"-Haltung die Entwicklung der Technik zu fördern, hemmt die Untätigkeit des Gesetzgebers diese vielmehr.

Allerdings sollte sich der Gesetzgeber auf eine vermittelnde Position beziehen. Umfassende Regelungen zu den datenschutzrechtlichen Herausforderungen von RFID wird er in Ermangelung der erforderlichen Flexibilität und der unzulänglichen Erkenntnisgrundlage zum jetzigen Zeitpunkt nicht erfolgreich vorgeben können. Die Gefahr übermäßiger Beschränkungen im wirtschaftlichen Bereich steht hierbei in einem diffizilen Verhältnis zu dem potenziell erreichbaren Schutzniveau für das informationelle Selbstbestimmungsrecht des Einzelnen.

Der erste Schritt zu mehr Klarheit setzt voraus, dass deutlich wird, wann traditionelles Datenschutzrecht anwendbar ist und wann nicht.[839] Hierfür muss sich der Gesetzgeber zwingend einer Überarbeitung des Begriffs der personenbezogenen Daten annehmen. Von dieser Entscheidung hängt maßgeblich ab, ob RFID spezifische Regelungen nötig sind oder ob eine Anpassung der unzulänglichen weil überholten traditionellen Datenschutzregeln erforderlich wird.

Sofern produktbezogene Identifikationsnummern nicht dem Regime des traditionellen Datenschutzrechts unterworfen werden sollen und die Definition der personenbezogenen Daten entsprechend angepasst worden ist, muss den Gefahren des Tracking und der Profilbildung anderweitig begegnet werden. Hierfür sollte der Ansatz einer regulierten Selbstregulierung verfolgt werden.

Dabei sind Anreize für die Wirtschaft zur Abgabe von sektor- bzw. anwendungsspezifischen Selbstverpflichtungen im Wege klarer gesetzlicher Vorgaben nötig, die den Rahmen für solche Maßnahmen der Selbstregulierung bieten. Der bereits vorhandene § 38a BDSG kann hier als Ausgangspunkt herangezogen werden. Es bedarf darüber hinaus allerdings spezieller Vorgaben für den Bereich RFID, die in einem Ausführungsgesetz bzw. normkonkretisierenden Vorschriften geregelt werden können. Die Überprüfung, regelmäßige Überarbeitung und erneute Überprüfung der zu schaffenden Selbstverpflichtungen muss durch die Datenschutzaufsichtsbehörden erfolgen, um eine wirksame Kontrolle des Ineinandergreifens von gesetzlichen Vorgaben und Umsetzung durch die Wirtschaft zu gewährleisten und Defizite aufzudecken.

In den Vorgaben zur Selbstregulierung sollte der Gesetzgeber Vorgaben zu folgenden Punkten schaffen:

- *Transparenz und Information* über die Verwendung von RFID: Hierzu können nach den Vorgaben der EU-Empfehlung und nach Vorbild der New-Yorker Gesetzgebung Hinweisschilder an auffälligen Orten verwendet werden. Weiterhin sind Vorgaben zur Kennzeichnungspflicht von Tags und Lesegeräten zu machen.
- *Privacy-by-Design* mittels *Privacy Enhancing Technologies*: Als programmatischer Leitfaden sollte der *Privacy-by-Design*-Grundsatz mit in eine gesetzliche Regelung aufgenommen werden. Konkrete Ausgestaltungen sind aber der Wirtschafft zu überlassen. Die Verwendung von *Privacy Enhancing Technologies* findet unter Zumutungsgesichtspunk-

[839] So auch *Huber*, MMR, 2006, 728 (734).

ten, die an eine Wirtschaftlichkeit anknüpfen wird, ihre Grenzen: Mit übermäßigen Vorgaben in diesem Bereich wird der Gesetzgeber die Wirtschaft zu sehr beschränken und die potenziellen technischen Entwicklungen im Bereich RFID ersticken.

- *Deaktivierung und Entfernung* von RFID-Tags: Die Deaktivierung bzw. Entfernung von RFID-Tags wird von der EU-Empfehlung jedenfalls für den Einzelhandelsbereich – den künftig wohl größten Anwendungsbereich für RFID – vorgeschlagen. Wie gesehen kann durch Deaktivierung bzw. Entfernung der Tags jedenfalls unautorisiertes Tracking und Profilbildung durch Dritte außerhalb des Machtbereichs der Tag ausgebenden Stelle verhindert werden. Allerdings werden auch gewünschte weitergehende Verwendungen der Tags verhindert. Die Möglichkeit die Tags unbeschadet zu lassen, sollte vor diesem Hintergrund jedem Betroffenen individuell verbleiben. Die von der EU-Empfehlung vorgeschlagene Regelung, die Tags standardmäßig zu deaktivieren bzw. entfernen aber bei ausdrücklicher Einwilligung des Betroffenen die Tags funktionsfähig zu belassen, erscheint mithin sinnvoll. Nicht übernommen werden sollte allerdings die von der EU-Empfehlung vorgesehene Ausnahme, dass RFID-Tags, von denen *wahrscheinlich* keine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten ausgehen, von der Pflicht zur Deaktivierung bzw. Entfernung ausgenommen sind. Eine solche Regelung stellte die Qualifizierung von RFID-Daten in die Entscheidungsgewalt der Unternehmen. Die Frage, von welchen Daten wahrscheinlich keine Gefahr für die Rechte des Betroffenen ausgeht, wird indes von der Wirtschaft anders beantwortet als von Betroffenenvertretern. Eine grundsätzliche Pflicht zur Deaktivierung oder Entfernung hat nur dann zu unterbleiben, wenn ausgeschlossen ist, dass die betreffenden RFID-Tags in den Endkundenbereich gelangen.
- Regelungen zu *Tracking und Profilbildung*: Ein generelles Verbot von Tracking und Profilbildung sollte nicht in eine gesetzliche Vorgabe für eine Selbstverpflichtung der Wirtschaft einfließen. Die Gefahren in diesem Bereich sind noch nicht konkret genug, als dass die mit einem solchen Verbot einhergehenden Einschränkungen der Rechte der betroffenen Unternehmen gerechtfertigt wären. Stattdessen sollte den Unternehmen aufgegeben werden, sich zu verpflichten, wann immer möglich auch eindeutige Identifikationsnummern so zu verkürzen, dass eine Identifikation des einzelnen Produkts und damit auch seines Besitzers nicht mehr möglich ist.

Ebenfalls zum Bereich der Selbstregulierung gehört die Weiterentwicklung des bereits in § 9a BDSG vorgesehen Datenschutzaudits. Auch hier fehlt es an klaren Regeln, wie Auditverfahren und anschließende Datenschutzzertifikate ausgestaltet sein sollen, um die erforderliche Einheitlichkeit herzustellen. Solche Regeln sind für eine umfassende Akzeptanz und damit den wirtschaftlichen Erfolg von Selbstregulierung unerlässlich. Hier sind insbesondere die Entwicklungen im Bereich eines EU-weiten Auditverfahrens zu berücksichtigen, zu dem die Kommission eine Machbarkeitsstudie über ein EU-weites System von Datenschutzgütesiegeln einschließlich einer Analyse seiner wirtschaftlichen und sozialen Auswirkungen plant.[840]

[840] Mitteilung der Kommission KOM(2007) 228 endgültig, oben Fn. 660, S. 11.

II. Handlungsempfehlung an die Branche

Die Verwender von RFID-Systemen sehen sich in einer ambivalenten Situation: Auf der einen Seite verspricht die Technologie immense wirtschaftliche Vorteile; auf der anderen Seite birgt ihre Einführung jedenfalls da, wo Endkunden mit ihr in Berührung kommen, zur Zeit mangels eindeutiger Vorgaben, wie mit den datenschutzrechtlichen Herausforderungen umgegangen werden soll, erhebliche Risiken. Der Wirtschaft ist vor diesem Hintergrund ein großes Maß an Eigeninitiative abverlangt.

Ganz klar und von der Branche längst erkannt ist, dass die datenschutzrechtlichen Herausforderungen von RFID nicht unterschätzt werden dürfen. Hierbei wirkt erschwerend, dass eine Prognoseentscheidung angestellt werden muss: Welche datenschutzrechtlichen Risiken verwirklichen sich in Zukunft und wie reagiert der Gesetzgeber hierauf. Aus wirtschaftlichen Gesichtspunkten ist immer zu bedenken, dass technische Standards von heute, morgen veraltet sein können. Nachträgliche Veränderungen der Sicherheitsverfahren in den heute aufzubauenden RFID-Infrastrukturen dürften einen sehr hohen Investitionsaufwand erfordern.[841] Diesem hemmenden Faktor durch die latente Gefahr der Entwertung beträchtlicher Infrastrukturinvestitionen aufgrund von Sicherheitsproblemen kann die Branche nur mit entsprechender Weitsicht begegnen. Der Einsatz von *Privacy Enhancing Technologies* im Rahmen der Umsetzung des zunehmend populären *Privacy-by-Design*-Ansatzes verspricht sich vor diesem Hintergrund auf lange Sicht auch in flächendeckend einzusetzenden und damit möglichst preisgünstig zu haltenden RFID-Tags auszuzahlen.

Transparenz und Information ist ebenfalls auch aus wirtschaftlichen Gesichtspunkten von erheblicher Relevanz und sollte von RFID anwendenden Unternehmen nicht als *goodwill* an der Gemeinschaft verstanden werden. Kundenakzeptanz ist ein wesentliches Kriterium für wirtschaftlichen Erfolg. Bereits aus diesem Grund sollten Unternehmen die Abläufe offen legen, die Daten über ihre Kunden betreffen, auch wenn es sich ihrer Meinung nach nicht um personenbezogene Daten i.S.d. traditionellen Definition handelt. Wenn Kunden informiert sind und ihnen alleine hierüber eine Wahlmöglichkeit gegeben wird, können Datenschutzskandale, wie sie in den letzten Jahren immer wieder aufgetreten sind, vermieden werden.

Darüber hinaus sollten sich RFID anwendende Unternehmen fragen, welche Daten sie tatsächlich sinnvoll nutzen können und so die Datenerhebungsvorgänge auf ein Minimum reduzieren. Damit werden nicht nur Ressourcen geschont – die Speicherung und Verwaltung von Daten erfordert Geld und Aufwand – sondern auch Datenhalden vermieden, denen immer das latente Risiko des Missbrauchs anhaftet.

III. Handlungsempfehlung an die Endnutzer

Den Endnutzern ist zu raten, was grundsätzlich gilt: Bestehende Möglichkeiten zur Kontrolle über die eigenen Daten sollten genutzt werden. Dies betrifft zum einen die Berücksichtigung

[841] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, oben Fn. 83, S. 99.

einer den eigenen Bedürfnissen angepassten Datenhygiene und andererseits die Wahrnehmung von Informationsangeboten. Wo traditionelles Datenschutzrecht anwendbar ist, stehen den Betroffenen zusätzlich Betroffenenrechte zu, die ebenfalls nach eigenen Bedürfnissen eingesetzt werden sollten.

Wie in anderen Bereichen gilt auch im Zusammenhang mit RFID: Einmal erhobene und gespeicherte Daten sind in einer informatisierten Welt wenn überhaupt nur mit größtem Aufwand wieder zurück zu holen, sprich zu löschen. Von daher sollte – wer ein möglichst großes Maß an Privatheit auch in Zukunft für sich in Anspruch nehmen will – die Preisgabe von Daten über sich selbst vermeiden, wo immer möglich. In RFID-Anwendungen heißt dies ganz klar: Tags sollten deaktiviert bzw. zerstört werden, sofern sie nicht mehr vom Betroffenen gebraucht werden. Hierfür muss sich der Betroffene zunächst darüber informieren, welche RFID-Tags er besitzt bzw. bei sich führt. Ohne entsprechende Informationen der Tag ausgebenden Stelle ist dies natürlich schwer umzusetzen. Klar ist aber, dass jedes Informationsangebot seitens der Tag ausgebenden Stelle nur so gut ist, wie das Interesse bei den Adressaten groß ist. Entsprechend wird es künftig immer wichtiger, dass Betroffene ein verstärktes Interesse am Verbleib von sie betreffenden Daten entwickeln.

In einigen Bereichen wird es nicht möglich sein, RFID-Tags zu deaktivieren oder entfernen, weil deren Funktionsfähigkeit faktisch oder sogar rechtlich vorausgesetzt wird. Dies ist beispielsweise bei Türöffnern der Fall oder auch bei mit RFID versehenen Ausweispapieren. Bei letzteren werden zwar aufwändige Verschlüsselungsmechanismen eingesetzt, die Missbrauch verhindern sollen. Eine hundertprozentige technische Sicherheit kann allerdings – wie immer – niemand gewähren. Wer für sich entscheidet, dass die Bemühungen im technischen Bereich sowie das eigene Vertrauen kein hinreichendes Sicherheitsgefühl schaffen, dem bleibt zuletzt der Griff zur Aluminiumhülle.

Literaturverzeichnis

Abel, Ralf-Bernd, Umsetzung der Selbstregulierung im Datenschutz: Probleme und Lösungen, RDV 2003, 11 ff.

Abel, Ralf-Bernd, 2.7 Geschichte des Datenschutzrechts *in:* Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, C.H. Beck München 2003

Albrecht, Katherine/ McIntyre, Liz, Spychips, Pearson New York 2005

Balkovic, Edward/ Bikson, Tora K./ Bitko, Gordon, 9 to 5: "Do You Know If Your Boss Knows Where You Are?", Case Studies of Radio Frequency Identification Usage in the Workplace, RAND Corporation, 2005 abrufbar unter http://www.rand.org/content/dam/rand/pubs/technical_reports/2005/RAND_TR197.pdf (04.04.2013)

Bowen Ayre, Lori, Wireless Tracking in the Library: Benefits, Threats, and Responsibilities *in:* Garfinkel, Simson/ Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Addison-Wesley Professional, Upper Saddle River, NJ (USA) 2006, S. 229-243

Brühann, Ulf, 2.4 Europarechtliche Grundlagen *in:* Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, C.H. Beck München 2003

Büllesbach, Alfred, Überblick über Europäische Datenschutzregelungen bezüglich des Datenaustauschs mit Ländern außerhalb der Europäischen Union, RDV 2002, 55

Damman, Ulrich/ Simitis, Spiros, EG-Datenschutzrichtlinie, Kommentar, Nomos, Baden-Baden, 1997

Däubler, Wolfgang/ Klebe, Thomas/ Wedde, Peter/ Weichert, Thilo (Hrsg.), Bundesdatenschutzgesetz – Kompaktkommentar zum BDSG, 3. Auflage, Bund Verlag, Frankfurt am Main, 2010, zitiert: *Bearbeiter* in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § … Rn. …

Dreier, Horst (Hrsg.), Grundgesetz Kommentar, Band 1, Art. 1-19, 2. Auflage, Mohr Siebeck Tübingen 2004

Fassbender, Bardo, Wissen als Grundlage staatlichen Handelns *in:* Isensee, Josef/ Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band IV, Aufgaben des Staates 3. Auflage, C.F. Müller, Heidelberg u.a., 2006

Finkenzeller, Klaus, RFID-Handbuch, Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 4. Auflage, Carl Hanser Verlag GmbH & CO. KG, München 2006 (nach Abgabe ist die 6. Auflage 2012 erschienen)

Fishkin, Kenneth P./ Lundell, Jay, RFID in Healthcare, *in:* Garfinkel, Simson/Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Addison-Wesley Professional, Upper Saddle River , NJ (USA) 2006, S. 211-228

Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005

Flörkemeier, Christian, EPC-Technologie – vom Auto-ID Center zu EPCglobal *in:* Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 87 – 100

Flörkemeier, Christian/ Langheinrich, Marc/ Fleisch, Elgar/ Mattern, Friedemann/ Sarma, Sanjay E. (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, Springer, Berlin, Heidelberg 2008

Flörkemeier, Christian/ Schneider, Roland/Langheinrich, Marc, Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols *in:* Hitomi Murakami/ Hideyuki Nakashima/ Hideyuki Tokuda/ Michiaki Yasumura (Hrsg.), Ubiquitious Computing Systems"; Revised Selected Papers from the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan, Lecture Notes in Computer Science, Vol. 3598, Springer-Verlag, Berlin 2005, S. 214-231

Frenz, Walter, Handbuch Europarecht, Band 4, Europäische Grundrechte, Springer Verlag, Berlin, Heidelberg, 2009

Garfinkel, Simson, RFID Payments at ExxonMobil, *in:* Garfinkel, Simson/ Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Addison-Wesley Professional, Upper Saddle River, NJ (USA) 2006, S. 179-187

Garfinkel, Simson/ Holtzman, Henry, Understanding RFID Technology, *in:* Garfinkel, Simson/ Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Addison-Wesley Professional, Upper Saddle River, NJ (USA) 2006, S. 15-36

Garfinkel, Simson/ Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Addison-Wesley Professional, Upper Saddle River, NJ (USA) 2006

Gerhards, Julia, (Grund-)Recht auf Verschlüsselung?, Reihe „Der elektronische Rechtsverkehr", hrsg. von Prof. Dr. Alexander Roßnagel in Zusammenarbeit mit dem TeleTrusT Deutschland e.V., Band 23, Nomos Verlagsgesellschaft, Baden-Baden 2010

Gillert, Frank/ Hansen, Wolf-Rüdiger, RFID RFID for the Optimization of Business Processes, John Wiley and Sons Ltd, West Sussex (England) 2008

Gola, Peter/ Schomerus, Rudolf, Bundesdatenschutzgesetz Kommentar, 10. Auflage, C.H. Beck Verlag München 2010

Grabitz, Eberhard/ Hilf, Meinhard (Hrsg.), Das Recht der Europäischen Union, 40. Auflage 2009, C.H. Beck München, zitiert: *Bearbeiter* in: Grabitz/Hilf (Hrsg.), Art. … Rn. …

Gräfin von Westerholt, Margot/ Döring, Wolfgang, Datenschutzrechtliche Aspekte der Radio Frequency Identification, CR 2004, 710

Heidrich, Joerg/ Wegener, Christoph, Sichere Datenwolken – Cloud Computing und Datenschutz, MMR 2010, 803 ff.

Heinrich, Claus (Hrsg.), RFID and Beyond, Wiley Publishing, Indianapolis (USA), 2005

Holznagel, Bernd/ Bonnekoh, Mareike, Radio Frequency Identification – Innovation vs. Datenschutz, MMR 2006, 17 ff.

Holznagel, Bernd/ Schumacher, Pascal, Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID-Chips, MMR 2009, 3

Hornung, Gerrit, RFID und datenschutzrechtliche Transparenz, MMR 2006, XX ff.

Huber, Andrea, Radiofrequenz-Identifikation – Die aktuelle Diskussion in Europa, MMR 2006, 728 ff.

Huber, Andrea, RFID in Europa – Auf dem Weg zu einer Regulierung des „Internet der Dinge", MMR 2008, VI

Isensee, Josef/ Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band VII, Freiheitsrechte, 3. Auflage, C.F. Müller Heidelberg u.a., 2009, zitiert: *Bearbeiter*, Kapitel *in:* HStR VII, 2009, § … Rn. …

Isensee, Josef/ Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band IV, Aufgaben des Staates, 3. Auflage, C.F. Müller, Heidelberg u.a., 2006, Zitiert: *Bearbeiter*, Kapitel *in:* HStR IV, 2006, § … Rn. …

Jarass, Hans D./ Pieroth, Bodo, Grundgesetz Kommentar, 11. Auflage, C.H. Beck München 2011

Juels, Ari, Technological Approaches to the RFID Privacy Problem, *in:* Garfinkel, Simson/ Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Upper Saddle River , NJ (USA) 2006, S.329-339

Klug, Christoph, Persönlichkeitsschutz beim Datentransfer in die USA – Die Safe-Harbor-Lösung, RDV 2000, 212 ff.

Koh, Robin/ Staake, Thorsten, Nutzen von RFID zur Sicherung der Supply Chain der Pharmaindustrie *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 161 - 176

Kreicker, Helmut, RFID-Technik in der Dementenversorgung – Herausforderung für das Betreuungsrecht, NJW 2009, 890

Kube, Hanno, § 148 Persönlichkeitsrecht *in:* Isensee, Josef/ Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band VII, Freiheitsrechte, C.F. Müller Heidelberg u.a., 2009

Kuner, Christopher, European Data Protection Law – Corporate Compliance and Regulation, 2. Auflage, Oxford University Press, New York (USA), 2007

Kürschner, Chris/ Condea, Cosmin/ Kasten, Oliver/ Thiesse, Frédéric, Discovery Service Design in the EPCglobal Network *in:* Flörkemeier, Christian/ Langheinrich, Marc/ Fleisch, Elgar/ Mattern, Friedemann/ Sarma, Sanjay E. (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, Springer, Berlin, Heidelberg 2008, S. 19-34

Lampe, Matthias/ Flörkemeier, Christian/ Haller, Stephan, Einführung in die RFID-Technologie *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 69-86

Langheinrich, Marc, Personal Privacy in Ubiquitous Computing – Tools and System Support, 2005, abrufbar unter http://www.vs.inf.ethz.ch/res/papers/langheinrich-phd-2005.pdf (04.04.2013)

Langheinrich, Marc, Die Privatsphäre im Ubiquitous Computing *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 329-362

Langheinrich, Marc, Gibt es in einer total informatisierten Welt noch eine Privatsphäre? *in:* Mattern, Friedemann (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Springer Berlin Heidelberg 2007, S. 233-264, abrufbar unter http://www.vs.inf.ethz.ch/res/papers/langhein-comp21-2007.pdf (04.04.2013)

Leupold, Andreas/ Glossner, Silke (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 2. Auflage, Verlag C.H. Beck München 2011, zitiert: Leupold/Glossner/*Bearbeiter*, Münchener Anwaltshandbuch IT-Recht, Teil …, Rn. …

Mattern, Friedemann (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, Springer Berlin Heidelberg 2007

Mattern, Friedemann, Die technische Basis für das Internet der Dinge *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 39-66

Maunz, Theodor/ Dürig, Günter (Hrsg.), Grundgesetz Kommentar, Band 1, Stand April 2010, C.H. Beck München, zitiert: *Bearbeiter* in: Maunz/Dürig, GG, Art. … Rn. …

Merten, Detlef/ Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte, Band 1, Entwicklungen und Grundlagen, C.F. Müller, Heidelberg 2004, zitiert: *Bearbeiter*, Kapitel *in:* HGR I, 2004, § … Rn. …

Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 3. Auflage, Nomos, Baden-Baden 2011, zitiert: *Bearbeiter* in: Meyer, Art., Rn. …

Meyerdierks, Per, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8

Mullen, Dan/ Moore, Bert, Automatic Identification and Data Collection: What the Future Holds *in:* Garfinkel, Simson/Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy. Addison-Wesley Professional, Upper Saddle River , NJ (USA) 2006, S. 3-13

Münch, Ingo von/ Kunig, Philip (Hrsg.), Grundgesetz-Kommentar, Band 1, Präambel, Art. 1-19, 5. Auflage, C.H. Beck München, 2000, zitiert: *Bearbeiter* in: v. Münch/Kunig, GG, Art. … Rn. …

Ossenbühl, Fritz, Grundsätze der Grundrechtsinterpretation *in:* Merten, Detlef/ Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte, Band 1, Entwicklungen und Grundlagen, C.F. Müller, Heidelberg 2004

Polenz, Sven, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, Universitätsverlag Chemnitz, 2009, abrufbar unter http://www.qucosa.de/fileadmin/data/qucosa/documents/5562/data/Dissertation.pdf (04.04.2013)

Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, C.H. Beck München 2003, zitiert: *Bearbeiter* in: Roßnagel, Hdb. DSR, Kap. … Rn. …

Roßnagel, Alexander, Digitale Ausweise, DuD 2005, 59 ff.

Roßnagel, Alexander, Datenschutz in einem informatisierten Alltag (2007), Gutachten im Auftrag der Friedrich-Ebert-Stiftung, abrufbar unter http://library.fes.de/pdf-files/stabsabteilung/04548.pdf (04.04.2013)

Roßnagel, Alexander, 1. Einleitung *in:* Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, C.H. Beck München 2003

Roßnagel, Alexander, 3.6 Konzepte der Selbstregulierung Mediendiensten *in:* Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, C.H. Beck München 2003

Roßnagel, Alexander, 7.9 Datenschutz in Tele- und Mediendiensten *in:* Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, C.H. Beck München 2003

Roßnagel, Alexander/Hornung, Gerrit, Biometrische Daten in Ausweisen, DuD 2005, 69 ff.

Roßnagel, Alexander/Hornung, Gerrit, Umweltschutz vs. Datenschutz? – Zu den Möglichkeiten eines datenschutzkonformen Einsatzes von RFID-Systemen zur Abfallerkennung, UPR 2007, 255 ff.

Roßnagel, Alexander/ Pfitzmann, Andreas/ Garstka, Hansjürgen, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001, abrufbar unter http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile (04.04.2013)

Rothensee, Matthias, User Acceptance of the Intelligent Fridge: Empirical Results from a Simulation *in:* Flörkemeier, Christian/ Langheinrich, Marc/ Fleisch, Elgar/ Mattern, Friedemann/ Sarma, Sanjay E. (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, Springer, Berlin, Heidelberg 2008, S. 123-139

Saeltzer, Gerhard, Sind diese Daten personenbezogen oder nicht? DuD 2004, 28 ff.

Sarma, Sanjay, A History of the EPC *in:* Garfinkel, Simson/ Rosenberg, Beth (Hrsg.), RFID: Applications, Security, and Privacy, Addison-Wesley Professional, Upper Saddle River, NJ (USA) 2006, S. 37-55

Schaar, Peter, Selbstregulierung und Selbstkontrolle – Auswege aus dem Kontrolldilemma?, DuD 2003, 421 ff.

Scheuch, Michael, Günstiger Drucker, teure Tinte, ZDFheute.de WISO Meldung vom 24.04.2006, http://www.tintenfuzzy.de/Wissen/LinkedDocuments/wiso2.pdf (04.04.2013)

Schliesky, Utz (Hrsg.), Gesetz über Personalausweise und den elektronischen Identitätsnachweis, Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel 2009, zitiert: *Bearbeiter* in: Schliesky, Gesetz über Personalausweise und den elektronischen Identitätsnachweis, § … Rn. …

Schmid, Viola, Mastering the Legal Challenges, *in:* Heinrich, Claus (Hrsg.), RFID and Beyond, S.193-207, Wiley Publishing, Indianapolis (USA), 2005

Schmid, Viola, Radio Frequency Identification Law Beyond 2007 *in:* Flörkemeier, Christian/ Langheinrich, Marc/ Fleisch, Elgar/ Mattern, Friedemann/ Sarma, Sanjay E. (Hrsg.), The Internet of Things, First International Conference, IOT 2008, Proceedings, Springer, Berlin, Heidelberg 2008, S. 196-213.

Schmid, Viola, RFID Law in a Global Perspective *in*: Gillert, Frank/ Hansen, Wolf-Rüdiger, RFID RFID for the Optimization of Business Processes, John Wiley and Sons Ltd, West Sussex (England) 2008, S. 209-219

Schmitt Glaeser, Walter, § 129 Schutz der Privatsphäre *in:* Isensee, Josef/ Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band VI Freiheitsrechte, C.F. Müller Heidelberg, 1989

Schröder, Christian, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, Nomos Verlag, Baden-Baden, 2007

Simchi-Levi, David, The Impact of RFID on Supply Chain Efficiency *in:* Heinrich, Claus (Hrsg.), RFID and Beyond, Wiley Publishing, Indianapolis (USA), 2005, S. 209-220

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 6. Auflage, Nomos Baden-Baden 2006, zitiert: *Bearbeiter* in: Simitis, BDSG, § … Rn. …

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 7. Auflage, Nomos Baden-Baden 2011, zitiert: *Bearbeiter* in: Simitis, BDSG (2011), § … Rn. …

Solove, Daniel J., Digital Person: Technology and Privacy in the Information Age, NYU Press New York (USA) 2006

Solove, Daniel J./ Schwartz, Paul M., Information Privacy Law, 3rd Edition, Aspen Publishers/Wolters Kluwer, New York (USA) 2009

SPIEGEL, Börse unter der Haut, Ausgabe 23/2004 vom 29.05.2004, S. 156

Stratford, Jean Slemmons/ Stratford, Juri, Data Protection and Privacy in the United States and Europe, abrufbar unter http://www.iassistdata.org/downloads/iqvol223stratford.pdf (04.04.2013)

Taeger, Jürgen/ Gabel, Detlev (Hrsg.), Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft GmbH, Frankfurt am Main 2010, zitiert: Taeger/Gabel/*Bearbeiter*, § … (Gesetz) Rn. …

Tellkamp, Christian/ Haller, Stephan, Automatische Produktidentifikation in der Supply Chain des Einzelhandels *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 225-249

Tellkamp, Christian/ Quide, Uwe, Einsatz von RFID in der Bekleidungsindustrie *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 143-160

Tettinger, Peter J./ Stern, Klaus, Kölner Gemeinschaftskommentar Europäische Grundrechtecharta, Verlag C.H. Beck, München, 2006, zitiert: *Bearbeiter* in: Tettinger/Stern, Art. …, Rn. …

Thielmann, Heinz/ Kuhlin, Bernd (Hrsg.), The Practical Real-Time Enterprise: Facts and Perspectives, Springer Berlin, 2005

Thiesse, Frédéric/ Gillert, Frank, Das smarte Buch *in:* Fleisch, Elgar/ Mattern, Friedemann (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visio-

nen, Technologien, Anwendungen, Handlungsanleitungen, Springer Berlin Heidelberg 2005, S. 291-299

Tiedemann, Paul, Von den Schranken des allgemeinen Persönlichkeitsrechts, DÖV 2003, 74 ff.

Tinnefeld, Marie-Theres/ Ehmann, Eugen/ Gerling, Rainer, Einführung in das Datenschutzrecht, 4. Auflage, Oldenbourg Verlag, München/Wien 2005 (nach Abgabe ist die 5. Auflage 2012 erschienen)

von Mangoldt, Hermann/ Klein, Friedrich/ Starck, Christian (Hrsg.), Kommentar zum Grundgesetz, Band 1, 6. Auflage Verlag Franz Vahlen München, München 2010, zitiert: *Bearbeiter* in: v. Mangoldt/Klein/Starck, GG I, Art. Rn.

von Münch, Ingo/ Kunig, Philip (Hrsg.), Grundgesetzt- Kommentar, Band 1, 5. Auflage, C.H. Beck, München 2000, zitiert: *Bearbeiter* in: v. Münch/Kunig, GG, Art. … Rn. …

Weichert, Thilo, Die Fußball-WM als Überwachungs-Großprojekt, 2005, abrufbar unter https://www.datenschutzzentrum.de/allgemein/wmticket.htm (04.04.2013)

EU-Rechtsakte

Europäische Kommission, Empfehlung 2009/387/EG vom 12.05.2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen, ABl. L 122/47 vom 16.05.2009, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF (04.04.2013)

Europäischer Rat, Verordnung (EG) Nr. 21/2004 des Rates vom 17. Dezember 2003 zur Einführung eines Systems zur Kennzeichnung und Registrierung von Schafen und Ziegen und zur Änderung der Verordnung (EG) Nr. 1782/2003 sowie der Richtlinien 92/102/EWG und 64/432/EWG, ABl. L 005 vom 09.01.2004, S. 8-17, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0021:DE:HTML (04.04.2013)

Europäischer Rat, Verordnung (EG) 2252/2004 des Rates vom 13. 12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. L 385 vom 29.12.2004 S. 1 ff., abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:de:HTML (04.04.2013)

Europäisches Parlament, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31 vom 23.11.1995, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML (04.04.2013)

Europäisches Parlament, Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. L 24/1 vom 30.01.1998, abruf-

bar unter http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=DE&numdoc=31997L0066&model=guichett (04.04.2013)

Europäisches Parlament, Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8/1 vom 12.1.2001, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:DE:PDF (04.04.2013)

Europäisches Parlament, Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201/37 vom 31.7.2002, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:de:HTML (04.04.2013)

Europäisches Parlament, Richtlinie 2009/136/ des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Erwägungsgrund 56, ABl. L 337 vom 18.12.2009, S. 11ff., abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:PDF (04.04.2013)

Öffentliche Dokumente EU

Artikel-29 Datenschutzgruppe, WP 37, Privatsphäre im Internet, vom 21. November 2000, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37de.pdf (04.04.2013)

Artikel-29-Datenschutzgruppe, WP 105, Arbeitspapier, Datenschutzfragen im Zusammenhang mit der RFID-Technik, 19.01.2005, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf (04.04.2013)

Artikel-29-Datenschutzgruppe, WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20.06.2007, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf (04.04.2013)

Artikel-29-Datenschutzgruppe, WP 175, Stellungnahme 5/2010 zum Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen, vom 13.07.2010, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_de.pdf (04.04.2013)

Artikel-29-Datenschutzgruppe, WP 180, Stellungnahme 9/2011 zu dem überarbeiteten Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-

Anwendungen, vom 11.02.2011, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_de.pdf (04.04.2013)

Europäische Kommission, Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung“, KOM(2006) 251 endgültig, vom 31.05.2006, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:DE:PDF (04.04.2013)

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zu „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“, KOM(2007) 96 endgültig, vom 15.03.2007, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:DE:PDF (04.04.2013)

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat „über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre“, vom 02.05.2007, KOM(2007) 228 endgültig, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:DE:PDF (04.04.2013)

Europäische Kommission, Beschluss der Kommission vom 28.06.2007 zur Einsetzung der Sachverständigengruppe für Funkfrequenzkennzeichnung (RFID), 2007/467/EG, ABl. L 176/25 vom 06.07.2007, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:0030:de:PDF (04.04.2013)

Europäische Kommission, Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 31.03.2010, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf (04.04.2013)

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endgültig, 04.11.2010, abrufbar unter http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf (04.04.2013)

Europäische Kommission, Consultation on the Commission's comprehensive approach on personal data protection in the European Union, abrufbar unter http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm (04.04.2013)

Europäische Kommission, Privacy and Data Protection Impact Assessment Framework for RFID Applications (nur in englischer Sprache), vom 12.01.2011, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf (04.04.2013)

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Der Schutz der Privatsphäre in einer vernetzten Welt - Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endgültig vom 25.01.2012, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:DE:PDF (04.04.2013)

Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr KOM(2012) 10 endgültig 25.01.2012, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:PDF (04.04.2013)

Europäische Kommission,Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig vom 25.01.2012, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF (04.04.2013)

Europäischer Datenschutzbeauftragter, Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ (KOM(2007) 96), 2008/C 101/01, ABl. C 101/1 vom 23.04.2008, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_DE.pdf (04.04.2013)

Europäischer Rat, Entschließung des Rates vom 22. März 2007 zu einer Strategie für eine sichere Informationsgesellschaft in Europa, 2007/C 68/01, Abl. C 68/1 vom 24.03.2007, abrufbar unter http://eur-lex.europa.eu/LexUriServ/site/de/oj/2007/c_068/c_06820070324de00010004.pdf (04.04.2013)

Europäisches Parlament, STOA Studie RFID and Identity Management in Everyday Life, 2007, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2007/383219/IPOL-JOIN_ET(2007)383219_EN.pdf (04.04.2013).

Öffentliche Dokumente Deutschland

Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2006 in Bremen, Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich: Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!, abrufbar unter

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/November06RFID.pdf?__blob=publicationFile (04.04.2013)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, Bonn 2004, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/RIKCHA_pdf.pdf?__blob=publicationFile (04.04.2013)

Bundesamt für Sicherheit in der Informationstechnik (BSI), TR 03126 – Technische Richtlinie für den sicheren RFID-Einsatz, TR 03126-1: Einsatzgebiet „eTicketing im öffentlichen Personenverkehr“, Bonn 2008, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03126/BSI-TR-03126-1_pdf.pdf;jsessionid=574B87E22A2867D6824C01896F12C9FF.2_cid156?__blob=publicationFile (04.04.2013).

Bundesministerium des Innern, Antworten auf den Fragenkatalog des Bundesministeriums der Justiz zur Online-Durchsuchung, vom 22.10.2007, abrufbar unter http://asset.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (04.04.2013)

Bundesministerium des Innern, Gesetzentwurf zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht vom 01.12.2010, abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile (04.04.2013)

Bundesministerium für Bildung und Forschung, TAUCIS, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung 2006, abrufbar unter http://www.bmbf.de/pubRD/ita_taucis.pdf (04.04.2013)

Bundesministerium für Wirtschaft und Technologie, European Policy Outlook RFID, 2007, abrufbar unter http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeuropeancommision/European_Policy_Outlock_RFID.pdf (04.04.2013)

Bundesnetzagentur, Informationsblatt „RFID, das kontaktlose Informationssystem“, abrufbar unter http://emf2.bundesnetzagentur.de/pdf/RFID-BNetzA.pdf (04.04.2013)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, Datenschutz-Kodex für Geodatendienste, Stand Dezember 2010, abrufbar unter http://www.bitkom.org/files/documents/Datenschutz_Kodex.pdf (04.04.2013)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, White Paper RFID – Technologie, Systeme und Anwendungen, 2005, abrufbar unter http://www.bitkom.org/files/documents/White_Paper_RFID_deutsch_11.08.2005__final.pdf (04.04.2013)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, Informationspapier „Radio Frequency Identification (RFID) in der Diskussion – Technik, Einsatzformen, Datenschutz“, 2004, abrufbar unter

http://www.bitkom.org/files/documents/BITKOM_RFID-Informationspapier_16.11.04.pdf (04.04.2013)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM, Pressemitteling vom 06.04.2011, Selbstverpflichtung zum Datenschutz bei RFID, abrufbar unter http://www.bitkom.org/de/themen/50792_67587.aspx (04.04.2013)

CDU, CSU, FDP, Koalitionsvertrag 2009, 17. Legislaturperiode, abrufbar unter http://www.cdu.de/doc/pdfc/091026-koalitionsvertrag-cducsu-fdp.pdf (04.04.2013)

Deutscher Bundesrat, Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 18.03.2011, abrufbar unter http://www.bundesrat.de/cln_228/SharedDocs/Drucksachen/2011/0001-0100/48-11_28B_29,templateId=raw,property=publicationFile.pdf/48-11%28B%29.pdf (04.04.2013)

Deutscher Bundesrat, Antrag des Landes Rheinland-Pfalz, Entschließung des Bundesrates zum verbrauchergerechten Einsatz der Radiofrequenztechnologie RFID, BRDrucks. 48/11 vom 03.02.2011, abrufbar unter http://www.bundesrat.de/cln_161/SharedDocs/Drucksachen/2011/0001-0100/48-11%2CtemplateId%3Draw%2Cproperty%3DpublicationFile.pdf/48-11.pdf (04.04.2013)

Deutscher Bundestag, Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze (BDSG-ÄndG 2001) in der Fassung des Innenausschusses des Bundestages vom 04.04.2001, BTDrucks 14/5793, abrufbar unter http://dip21.bundestag.de/dip21/btd/14/057/1405793.pdf (04.04.2013)

Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Rainer Brüderle, Ernst Burgbacher, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/3025 – Technologie der Radio Frequency Identification, BTDrucks. 15/3190 vom 26. 05. 2004 abrufbar unter http://dipbt.bundestag.de/dip21/btd/15/031/1503190.pdf (04.04.2013)

Deutscher Bundestag, Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie, BTDrucks 16/7891 vom 23.01.2008, abrufbar unter http://dip21.bundestag.de/dip21/btd/16/078/1607891.pdf (04.04.2013)

Deutscher Bundestag, Antrag der Fraktion der FDP, Datenschutz im nicht öffentlichen Bereich verbessern, BTDrucks 16/9452 vom 04.06.2008, abrufbar unter http://dip21.bundestag.de/dip21/btd/16/094/1609452.pdf (04.04.2013)

Deutscher Bundestag, Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BTDrucks 16/12011 vom 18.02.2009, abrufbar unter http://dipbt.bundestag.de/dip21/btd/16/120/1612011.pdf (04.04.2013)

Deutscher Bundestag, Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss), BTDrucks 16/13657 vom 01.07.2009, abrufbar unter http://dipbt.bundestag.de/dip21/btd/16/136/1613657.pdf (04.04.2013)

Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Nicole Maisch, Dr. Konstantin von Notz, Markus Tressel, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/6797 – Erfüllung des Koaliti-

onsvertrags und von Ankündigungen der Bundesregierung im Hinblick auf verbraucherpolitische Vorhaben, BTDrucks. 17/6881vom 01. 09. 2011, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/068/1706881.pdf (04.04.2013)

Deutscher Bundestag, Zwischenbericht der Enquête-Kommission „Internet und Digitale Gesellschaft“ zum Thema Datenschutz vom 17.10.2011, abrufbar unter http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20111212/Ausschussdrucksache_17_24_42.pdf (04.04.2013)

Deutscher Bundestag, Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Technologie, BTDrucks 17/7521, vom 26.10.2011, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/075/1707521.pdf (04.04.2013)

Deutscher Bundestag, Beschlussempfehlung des Vermittlungsausschusses, BTDrucks 17/8569, vom 08.02.2012, abrufbar unter http://dipbt.bundestag.de/dip21/btd/17/085/1708569.pdf (04.04.2013)

GS1 Germany, RFID Daten- und Verbraucherschutz, Positionspapier der deutschen Wirtschaft, Stand Juni 2006, abrufbar unter http://www.gs1-germany.de/common/downloads/epc_rfid/3001_daten_verbraucherschutz.pdf (04.04.2013)

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken, Entschließung zu Radio-Frequency Identification vom 20.11.2003, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/67DSK-Radio-Frequency-Identification.pdf?__blob=publicationFile (04.04.2013)

Konferenz der Datenschutzbeauftragten, Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg, Verbindliche Regelungen für den Einsatz von RFID-Technologien abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/72DSK-RFID.pdf?__blob=publicationFile (04.04.2013)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kundenbindungssysteme und Datenschutz (Gutachten), abrufbar unter: https://www.datenschutzzentrum.de/wirtschaft/Kundenbindungssysteme.pdf (04.04.2013)

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBud e.V.), Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, vom 14.11.2003/19.11.2003, abrufbar unter http://www.foebud.org/rfid/unsere-positionen (04.04.2013)

Öffentliche Dokumente USA

U.S. Department for Homeland Security (DHS), Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, “Minimum Standards for Driver’s licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes”, abrufbar unter http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (04.04.2013)

U.S. Food and Drug Administration, Counterfeit Drug Task Report February 2004, abrufbar unter http://www.fda.gov/Drugs/DrugSafety/ucm173297.htm (04.04.2013)

U.S. Food and Drug Administration, Doc. No. 2004N–0477, Medical Devices; General Hospital and Personal Use Devices; Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information, Federal Register, Vol. 69, No. 237, vom 10.12.2004, abrufbar unter http://www.fda.gov/ohrms/dockets/98fr/04-27077.pdf (04.04.2013)

U.S. Food and Drug Administration, Doc. 1541 vom 10.12.2004, Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information, abrufbar unter http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm072141.htm (04.04.2013)

Sonstige öffentliche Dokumente

Europarat, Konvention zum Schutze der Menschenrechte und Grundfreiheiten (SEV Nr. 005), vom 4. November 1950, abrufbar unter http://www.echr.coe.int/NR/rdonlyres/F45A65CD-38BE-4FF7-8284-EE6C2BE36FB7/0/GER_CONV.pdf (04.04.2013)

Europarat, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS Nr. 108), vom 28. Januar 1980, abrufbar unter http://conventions.coe.int/treaty/ger/treaties/html/108.htm (04.04.2013)

GS1, Guidelines on EPC for Consumer Products, Stand September 2005, abrufbar unter http://www.gs1.org/epcglobal/public_policy/guidelines (04.04.2013)

International Civil Aviation Organization (ICAO), Doc. 9303, Machine Readable Travel Documents, 6th edition 2006, abrufbar unter http://www.icao.int/publications/Documents/9303_p1_v1_cons_en.pdf (04.04.2013)

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, vom 23. September 1980, abrufbar unter http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html (04.04.2013)

United Nations Organisation, Richtlinien betreffend personenbezogene Daten in automatisierten Dateien vom 14. Dezember 1990 (A/RES/45/95), abrufbar (englisch) unter http://www.un.org/documents/ga/res/45/a45r095.htm (04.04.2013)

Sonstige Online-Quellen

BBC News, Meldung vom 25.09.2003, Smart Cards Track Commuters, abrufbar unter http://news.bbc.co.uk/2/hi/technology/3121652.stm (04.04.2013)

BBC News, Meldung vom 13.03.2006, Oyster data is 'new police tool', abrufbar unter http://news.bbc.co.uk/1/hi/england/london/4800490.stm (04.04.2013)

c't Magazin 23/06, Operation RFID-Tag startet in Ungarn – RFID- und Videotechnik unterstützen einander bei der Flughafenüberwachung, abrufbar unter

http://www.heise.de/ct/artikel/Operation-RFID-Tag-startet-in-Ungarn-290732.html (04.04.2013)

C&A Pressemitteilung vom 01.06.2012, abrufbar unter http://www.c-and-a.com/de/de/corporate/fileadmin/mediathek/de-de/Pressemitteilungen/C-und-A_startet_RFID-Projekt_an_f%C3%BCnf_Standorten.pdf (04.04.2013)

CASPIAN, Pressemitteilung 12.03.2003, Consumer Group Calls for Immediate Worldwide Boycott of Benetton, abrufbar unter http://www.nocards.org/press/pressrelease03-12-03.shtml (04.04.2013)

CBS News, Meldung vom 11.10.2004, Japanese Kids get Radio ID'd, abrufbar unter http://www.cbsnews.com/stories/2004/10/11/tech/main648681.shtml (04.04.2013)

Heise News Meldung, vom 02.02.2004, RFID beim Einkaufen: Danke, Katherine, abrufbar unter http://www.heise.de/newsticker/meldung/44237 (04.04.2013)

Heise News Meldung, vom 27.02.2004, Metro zieht RFID-Karte zurück, abrufbar unter http://www.heise.de/newsticker/meldung/45062 (04.04.2013)

Heise News Meldung, vom 02.11.2004, Nokia stellt RFID-Handy-Hülle vor und testet Ticket-Verkauf, abrufbar unter http://www.heise.de/newsticker/meldung/Nokia-stellt-RFID-Handy-Huelle-vor-und-testet-Ticket-Verkauf-112574.html (04.04.2013)

Heise News Meldung, vom 10.02.2006, Firma markiert Mitarbeiter per RFID, abrufbar unter http://www.heise.de/newsticker/meldung/69438/ (04.04.2013)

Heise News Meldung, vom 24.11.2006, Berührungsloses Zahlen mit Visa ab 2007 auch in Europa, abrufbar unter http://www.heise.de/newsticker/meldung/Beruehrungsloses-Zahlen-mit-Visa-ab-2007-auch-in-Europa-120901.html (04.04.2013)

Heise News Meldung, vom 10.09.2007, Karstadt führt RFID-Etiketten ein, abrufbar unter http://www.heise.de/newsticker/meldung/95771 (04.04.2013)

Heise News Meldung, vom 11.09.2007, Krebsverdacht bei implantierten RFID-Chips, abrufbar unter http://www.heise.de/newsticker/Krebsverdacht-bei-implantierten-RFID-Chips--/meldung/95797 (04.04.2013)

Heise News Meldung, vom 09.10.2007, SPD gibt Widerstand gegen Fingerabdrücke in Personalausweisen auf, http://www.heise.de/newsticker/meldung/97138 (04.04.2013)

Heise News Meldung, vom 21.10.2007, Britische Schule testet RFID-Chips in der Schulkleidung, abrufbar unter http://www.heise.de/newsticker/meldung/97700 (04.04.2013)

Heise News Meldung, vom 23.11.2007, Mastercard bringt drahtloses Bezahlen nach Deutschland, abrufbar unter http://www.heise.de/newsticker/meldung/Mastercard-bringt-drahtloses-Bezahlen-nach-Deutschland-Update-198726.html (04.04.2013)

Heise News Meldung, vom 15.05.2011, BSI verärgert Ärzte, abrufbar unter http://www.heise.de/newsticker/meldung/BSI-veraergert-Aerzte-1243157.html (04.04.2013)

Heise News Meldung, vom 29.06.2011, Datenschützer warnen vor flächendeckender Gesichtserkennung, abrufbar unter http://www.heise.de/newsticker/meldung/Datenschuetzer-warnen-vor-flaechendeckender-Gesichtserkennung-1269926.html (04.04.2013)

Heise News Meldung, vom 19.10.2011, Galaxy Nexus: Google-Handy mit HD-Display und Android 4.0, abrufbar unter http://www.heise.de/mobil/meldung/Galaxy-Nexus-Google-Handy-mit-HD-Display-und-Android-4-0-1363207.html (04.04.2013)

Heise News Meldung, vom 15.11.2011, NFC-Nachrüstsatz für Handys, abrufbar unter http://www.heise.de/newsticker/meldung/NFC-Nachruestsatz-fuer-Handys-1379208.html (04.04.2013)

Heise News Meldung, vom 16.01.2012, Funketiketten in der Kritik, abrufbar unter http://www.heise.de/newsticker/meldung/Funketiketten-in-der-Kritik-1414110.html (04.04.2013)

RFID Journal, Meldung vom 28.03.2003, Metro Opens 'Store of the Future, abrufbar unter http://www.rfidjournal.com/article/articleview/399/1/1 (04.04.2013)

RFID Journal, Meldung vom 19.06.2006, Active RFID Drills into Mining Industrie, abrufbar unter http://www.rfidjournal.com/article/view/6517 (04.04.2013)

RFID Journal, Meldung vom 18.08.2006, Air France-KLM Embarks on RFID Luggage-Tag Trial, abrufbar unter http://www.rfidjournal.com/article/articleview/2600/1/1 (04.04.2013)

RFID Journal, Meldung vom 30.04.2008, In German Courts, RFID Dictates Where Audio Files Are Stored, http://www.rfidjournal.com/article/articleview/4059/1/1/ (04.04.2013)

RFID Journal, Meldung vom 30.05.2008, Copenhagen Airport Pilots RFID-Tags for Passengers, abrufbar unter http://www.rfidjournal.com/article/articleview/4104/1/1/ (04.04.2013)

Seattle Post Intelligencer Online, Meldung vom 23.03.2007, New driver's license OK'd for border, abrufbar unter http://seattlepi.nwsource.com/local/308864_border24.html (04.04.2013)

Sensors, Meldung vom 01.02.2004, When Safety Matters: Using Active RFID Down in the Mines, abrufbar unter http://www.sensorsmag.com/sensors/article/articleDetail.jsp?id=319650 (04.04.2013)

Silicon.de news, Meldung vom 09.02.2004, RFID ist für Verbraucher ein Buch mit sieben Siegeln, abrufbar unter http://www.silicon.de/enid/storage_network/6464 (04.04.2013)

The Wall Street Journal, Meldung vom 28.03.2011, Google Sets Role in Mobile Payment, abrufbar unter http://online.wsj.com/article/SB10001424052748703576204576226722412152678.html?KEYWORDS=google+android (04.04.2013)

Abkürzungsverzeichnis

a.A.	andere/r Ansicht
ABl.	Amtsblatt
Abs.	Absatz
ÄndG	Änderungsgesetz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BRDrucks	Bundesratsdrucksache
BTDrucks	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des BVerfG
BVerfGK	Kammerentscheidungen des BVerfG
bzgl.	bezüglich
bzw.	beziehungsweise
CR	Zeitschrift Computer und Recht
d.h.	das heißt
DÖV	Die Öffentliche Verwaltung
DuD	Datenschutz und Datensicherheit
EG	Vertrag über die Europäischen Gemeinschaften
etc.	et cetera
EU	Vertrag über die Europäische Union
EuGH	Gerichtshof der Europäischen Gemeinschaften
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f.	folgende
ff.	fortfolgende
Fn.	Fußnote
gem.	gemäß
ggf.	gegebenenfalls
GRCh	Europäische Grundrechtechrata
grds.	grundsätzlich
GVBl	Gesetz- und Verordnungsblatt
Hdb.	Handbuch
Hrsg.	Herausgeber
Hs.	Halbsatz
HSOG	Hessisches Sicherheits- und Ordnungsgesetz

i.R.d.	im Rahmen der/des
i.R.v.	im Rahmen von
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
LDSGe	Landesdatenschutzgesetze
MMR	Multimedia und Recht
m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht Rechtsprechungsreport
o.ä.	oder ähnliches
PassG	Passgesetz
PAuswG	Personalausweisgesetz
RDV	Zeitschrift Recht der Datenverarbeitung
RFID	Radiofrequenzidentifikation/ Radio Frequency Identification
Rn.	Randnummer
Rspr.	Rechtsprechung
S.	Seite, Satz
s.o.	siehe oben
sog.	so genannte/n
s.u.	siehe unten
TMG	Telemediengesetz
TKG	Telekommunikationsgesetzt
u.a.	unter anderem; und andere
UPR	Zeitschrift für Umwelt- und Planungsrecht
Urt.	Urteil
v.	von, vom
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung
z.B.	zum Beispiel
ZUM	Zeitschrift für Urheber- und Medienrecht